



Australian
Competition &
Consumer
Commission

ACCC Report

Targeting scams

Report of the ACCC on scams activity 2014

May 2015

Foreword



Delia Rickard

The Australian Competition and Consumer Commission's (ACCC) sixth annual report on scams activity in Australia highlights the significant harm that scams continue to cause to the Australian community.

In 2014 nearly 92 000 scam-related contacts were received by the ACCC, almost the same as 2013. However, for the second consecutive year, reported financial losses decreased, with a total of nearly \$82 million being reported lost. This represents a fall of approximately 8 per cent. There was also a decrease in the number of people reporting losses with only 12 per cent compared to 14 per cent of total contacts in the previous year.

Both of these improvements are pleasing and hopefully reflect a greater awareness by Australians of scam activity. However, actual losses are likely to be much higher than what is reported to the ACCC—people report scams to a number of agencies, some don't recognise that they have fallen for a scam, and unfortunately many others are too embarrassed to report their experience.

As shown by this year's report, increasingly scams are targeting the online environment, with the internet fast on track to become the number one method of scams delivery. If scammers aren't after your money, then they're looking for your personal information. In 2014 losses reported to computer hacking scams doubled when compared with 2013 and other identity theft scams continued to be reported in significant numbers. Not only do we see increased levels of directly reported identity theft but we also see the deliberate misuse of personal information underpinning several of the scam categories where major financial losses are reported. For this reason, the 2015 consumer fraud week will ask Australians to 'get smarter with their data' and consider how secure their personal information really is.

Many of us are guilty of failing to take appropriate measures to safeguard our personal information. We live in a society that values our rights to privacy and has many laws in place to protect these. Consequently, we become complacent and often fail to put in place adequate safeguards to protect our personal information. Because of our increasing involvement in a global economy through online trade and commerce, it is more important than ever that we take steps to protect our personal information from those that seek to take advantage of our trust and the anonymity of digital communication to engage in fraudulent activity.

There is an element of trust in all transactions—trust that each party will carry out their end of the bargain, trust that each will act in good faith and, in an online environment, trust that people are who they say they are. Scammers understand this too well. They exploit the anonymity of the online world to avoid detection, steal information to create false identities and prey on the good name of major businesses to lend credence to their fraud. With these ends in mind, your personal information becomes an invaluable commodity and people will go to great lengths to acquire it.

In 2014 hacking, phishing and identity theft scams accounted for over \$3.5 million dollars which is only 4 per cent of total losses but represented more than a quarter of the 91 637 contacts reported to the ACCC. The percentage of those reporting losses may be low but this is often because the information garnered is used in a different, more elaborate fraud that takes place at some later point in time.

So many of the scams reported to the ACCC are underpinned by some aspect of identity fraud. Fake trader websites, classified advertisement scams, investment scams, online dating scams, reclaim scams and charity scams, to name a few. All of these scams rely on convincing their victims they are who they say they are.

Scammers will not only steal information but also buy information to target their victims. A multi-agency taskforce investigation targeting investment scams, conducted in 2011, revealed that fraudsters purchased lead lists from legitimate marketing companies to identify likely investors. There are also black markets where identity information is commonly bought and sold. A recent government report¹ on identity theft indicated that 'the price of fraudulent identity credentials ranges from around \$80 for Medicare cards to around \$350 for driver licences and \$1500 for an Australian passport to be altered by a professional document forger or up to \$20 000–\$30 000 for a legitimately issued passport with fraudulent details.

¹ Attorney-General's Department, *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot, 2014*

This year's report discusses the breadth and range of scams reported to the ACCC and examines how identity theft plays a role. In addition to going online to connect with victims, 2014 data also suggests that scammers are getting better at stealing people's personal details and money online. While online scams remained second to phone scams in terms of overall scam delivery levels, they caused the most financial harm—over \$47 million was reported lost via this approach. In 2015 the ACCC will continue its on-going educational efforts and support the Australasian Consumer Fraud Taskforce's 2015 Fraud Week campaign, 'get smarter with your data'.

There is a common misconception that scam victims are only the greedy and gullible. Anyone can fall victim to a scam and we are all vulnerable at some time in our lives to those unscrupulous individuals willing to take advantage of our better nature or simple mistakes. Often those sending money to scammers do so as a genuine desire to help someone they perceive to be in need of assistance. Charity scams and dating scams are but two examples of scammers preying on our good nature to perpetrate their fraud.

In 2014 the ACCC directed efforts at relationship scams which cause the most harm to victims. The good work that was commenced in 2014 will continue in 2015. The ACCC's Scam Disruption project used financial intelligence to identify those sending funds to high risk jurisdictions and warned them of the likelihood they were a victim of a scam. Of those that were subsequently confirmed as victims, 75 per cent were involved in online dating scams. With an increase in reported losses for online dating scams to over \$28 million in 2014, it is imperative we continue to focus on alerting potential victims to the pitfalls of this devastating scam. Early results from the ACCC Scams Disruption project are promising with 70 per cent of those that were sent a letter, warning of the perils of sending funds offshore, ceasing to send funds for at least a six week period.

The global nature of today's scams can frustrate law enforcement efforts, which is why education and awareness raising is a key pillar in scams prevention. It is pleasing to observe that the ACCC's SCAMwatch website continues to grow year on year as a resource turned to by the public, with visits to the site increasing by 9 per cent in 2014 to 1 336 869 unique visitors. The SCAMwatch free radar alert service also increased by 24 per cent in 2014 to just over 36 000 subscribers. The ACCC will continue its efforts to help Australians protect themselves against scams through educational initiatives. SCAMwatch will undergo a major facelift in 2015 but the SCAMwatch radar alert service will continue.

While scammers are professionals at evading the law, the ACCC does and will relentlessly pursue those that ignore court rulings and continue in their endeavours to rip off the Australian public. In 2014 the ACCC successfully took court action to bring Peter Foster to justice after years of misleading consumers and businesses with dodgy claims of money to be made selling dubious weight loss solutions.

The ACCC is also determined to find other innovative ways to counter scammers' evasive behaviour, with disruption a key tool in this approach. The ACCC's work is assisted by the Australasian Consumer Fraud Taskforce which comprises a number of government, business and community group partners that also play an important role in raising community awareness. The ACCC looks forward to working with the Taskforce to find better ways to disrupt scam activity and explore opportunities for working with intermediaries in industry whose services are exploited by scammers. Results of the ACCC's 2014 internet sweep of dating sites were mixed and point to the need for greater efforts within that industry to adopt better practices to protect their customers. Working again with the online industry to review and promote the Best Practice Guidelines will therefore be another area of focus for 2015. It really does make good business sense for organisations to invest time and effort into minimising fraud occurring through their services or platforms.

We hope that this report and the work of the ACCC in coming years helps Australians avoid scams and reinforces the need for them to safeguard their personal information and 'get smarter with their data'.

Delia Rickard

*Deputy Chair, Australian Competition and Consumer Commission
Chair, Australasian Consumer Fraud Taskforce*

Contents

| | |
|---|-----------|
| Foreword | i |
| 1. Snapshot of 2014 | 1 |
| 2. Scam contacts and trends | 4 |
| 2.1 Scam contact levels | 4 |
| 2.2 Financial losses to scams | 4 |
| 2.3 Scam delivery methods | 8 |
| 2.4 Demographics | 11 |
| 2.5 Conversion rates | 14 |
| 3. Disruption and enforcement activities | 18 |
| 3.1 Scam disruption activities | 18 |
| 3.2 Scam-related enforcement activities | 22 |
| 4. The top 10: 2014's most significant scams | 24 |
| 4.1 Overview of most common scam types reported to the ACCC | 24 |
| 4.2 The top 10 scams in 2014 (\$ reported loss) | 25 |
| #1. Dating and romance scams | 27 |
| #2. Investment scams | 31 |
| #3. Computer prediction software and sports investment schemes | 34 |
| #4. Inheritance scams | 36 |
| #5. Computer hacking scams | 38 |
| #6. Nigerian scams | 40 |
| #7. Fake trader websites | 42 |
| #8. Classified scams | 45 |
| #9. Unexpected prize and lottery scams | 47 |
| #10. Overpayment Scams | 50 |
| 5. Research | 51 |
| 5.1 Australian Institute of Criminology research | 51 |
| 5.2 Attorney-General's Department: Identity security | 51 |
| 5.3 Upcoming Australian Bureau of Statistics' personal fraud survey | 52 |
| 6. Education and awareness raising initiatives | 53 |
| 6.1 SCAMwatch | 53 |
| 6.2 Other scams educational resources | 55 |
| 6.3 Media and communications activity | 56 |
| 7. Domestic and international collaboration | 57 |
| 7.1 The Australasian Consumer Fraud Taskforce | 57 |
| 7.2 The International Consumer Protection and Enforcement Network | 59 |
| 7.3 Australian Transaction Reports and Analysis Centre partnership | 60 |
| 7.4 Australian Cybercrime Online Reporting Network (ACORN) | 60 |
| Appendix 1: Glossary of scam terms | 61 |
| Appendix 2: Scam tables by state and territory | 64 |
| Appendix 3: SCAMwatch radars | 72 |
| Appendix 4: Other scam-related educational materials | 74 |

ISBN 978 1 922145 50 5

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Commonwealth of Australia 2015

This work is copyright. In addition to any use permitted under the *Copyright Act 1968*, all material contained within this work is provided under a Creative Commons Attribution 3.0 Australia licence, with the exception of:

the Commonwealth Coat of Arms

the ACCC and AER logos

any illustration, diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright, but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 3.0 AU licence.

Requests and inquiries concerning reproduction and rights should be addressed to the Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601, or publishing.unit@accg.gov.au.

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

Parties who wish to re-publish or otherwise use the information in this publication must check this information for currency and accuracy prior to publication. This should be done prior to each publication edition, as ACCC guidance and relevant transitional legislation frequently change. Any queries parties have should be addressed to the Director, Corporate Communications ACCC, GPO Box 3131, Canberra ACT 2601, or publishing.unit@accg.gov.au.

ACCC 05/15_965

www.accc.gov.au

1. Snapshot of 2014

Overall contacts levels and financial losses

- In 2014 the ACCC continued to observe a high level of scams activity in Australia, with 91 637 scam-related contacts received from consumers and businesses compared with 91 927 in 2013.
- Scam losses reported to the ACCC totalled \$81 832 793, continuing a slight downward trend with an 8 per cent decrease from 2013 (\$89 136 975). This is a continuation of a reversal in the trend from 2010 through to 2012 where large annual increases in reported losses were observed. However, actual losses are likely to be higher as many scams go unreported and the ACCC is only one of several agencies that receive scam reports.

Most significant scams

- Similar to previous years, the majority of people contacting the ACCC about scam-related activities in 2014 (almost 88 per cent) reported no financial loss. Over one third of people who lost money reported losing between \$100 and \$499, which indicates scammers continue to prefer 'high volume low value scams'—that is, scams that are delivered to large numbers of recipients but cause smaller amounts of loss per victim.
- At the same time, the ACCC continued to receive reports of individuals suffering significant losses. Over 10 per cent of scam contacts reported losing above \$10 000 and there were 14 instances where losses exceeded \$500 000. There were no losses above \$1 million reported in 2014.
- The most damaging scams in terms of monetary loss continue to be those scams previously categorised as advance fee fraud and dating and romance scams which often evolve into advance fee fraud.
- In 2014 dating and romance scams remained in the number one position in terms of financial losses, with \$27 904 562 reported lost which accounts for 34 per cent of all reported losses. For the fourth consecutive year the ACCC has observed a decrease in the conversion rate of people who responded to an approach by a scam admirer and subsequently lost money—from 48 per cent in 2011 to 41 per cent in 2014. However, financial losses continue to remain substantially disproportionate to contacts, with dating and romance scams making up only 3 per cent of all scam-related contacts in 2014.
- The next most significant scam groups were investment fraud and computer prediction software scams, both of which are often dressed up as investment opportunities. Together they accounted for 26 per cent of reported losses and over \$21 million dollars. A further \$10 million of losses were reported against other types of advance fee fraud.
- In terms of numbers of scam reports to the ACCC in 2014, the top scams under the new classification system are reclaim scams, phishing, remote access scams and identity theft scams. Reclaim and remote access scams are new categories and 2013 figures are not available for these categories. Phishing, identity theft and hacking scams remained consistent with 2013 figures. The 25 504 contacts recorded in these scam categories suggests that scammers continue to value personal information that they can then use for other fraudulent activity and later financial gain.

Age range and location demographics

- At the end of 2013 the ACCC updated its data collection process. Demographic data for 2014 is significantly better than that previously recorded.
- Except for people aged under 24 (less than 9 per cent of reports), scam reports are fairly consistent across the different age categories.
- Gender was relatively evenly split with almost 55 per cent of reports from females and 45 per cent from males.
- The greatest number of scam reports came from New South Wales, Victoria and Queensland. Contact levels and associated losses were largely consistent with the percentage of the Australian population by state and territory.

Scam delivery method

- In 2014 over half (53 per cent) of scams were delivered via phone and text message, with combined total financial losses of \$23 470 222. Telephone calls remained the most popular delivery method, with 44 411 contacts and losses totalling \$21 499 957. Reports of scams delivered by text message decreased by almost 50 per cent, but reported losses remained at just under \$2 000 000.
- While the total loss figure is down for scams delivered by telephone and text by almost \$6 000 000 on 2013 losses, there was a corresponding rise in total losses for scams delivered online. This may be due to changes in classification that now record mobile app and social networking scams that are included in online scams but often delivered by telephone. Despite representing a lower percentage of contacts (38 per cent), scams delivered online caused the greatest financial harm with associated losses totaling \$47 387 308.
- While the number of reports of scams delivered via email remained approximately the same as 2013, financial losses increased by 55 per cent to \$19 180 568. It is not clear why this significant increase in losses has occurred and may simply reflect a return to loss levels seen in 2012, suggesting reported losses in 2013 for this category were unusually low.

The ACCC's education and awareness raising activities

- The ACCC continued to educate the public about how to identify and avoid scams, and raise community awareness about current scams targeting Australians. SCAMwatch, the Australian Government's website for information about scams that is run by the ACCC, received 1 336 869 unique visitors in 2014, an increase of 9 per cent from the previous year.
- The ACCC also continued to issue free SCAMwatch radar alerts to its subscription base, which in 2014 increased by 24 per cent to reach 36 165 subscribers. A total of 17 SCAMwatch alerts were issued warning about current scams, including joint radars issued with other government agencies and companies about scammers misusing consumer trust in these well-known entities.
- The ACCC's SCAMwatch_gov Twitter profile also continued to communicate with its 7721 followers in real time as scams emerged, with 539 tweets posted during the year.
- The 2014 National Consumer Fraud Week campaign, 'Know who you're dealing with' (16–22 June), received significant media coverage as the ACCC and the Australasian Consumer Fraud Taskforce asked Australians to take a step back and think about whether someone they met online is the real deal, particularly if they ask for money.
- *The Little Black Book of Scams* is the ACCC's most popular publication and 108 943 copies were distributed in 2014. A new small business scams factsheet was also produced.

The ACCC's collaboration, disruption and enforcement activities

Collaboration

- In 2014 the ACCC continued to chair the Australasian Consumer Fraud Taskforce, and coordinated with members and partners the 2014 Fraud Week Campaign 'know who you're dealing with' to raise community awareness about scams.

Disruption

- The ACCC's Scams Disruption Project commenced in August 2014 and will remain a compliance and enforcement priority in 2015. The project involves the use of financial intelligence to identify Australians sending funds to high risk jurisdictions who are then advised they may have been targeted by a scam. Just over 2000 letters were sent in the period August to December 2014 encouraging recipients to contact the ACCC to discuss their situation on a confidential basis. Of those that contacted the ACCC, 75 per cent were confirmed as scam victims.
- Early results show that 70 per cent of those receiving the ACCC's warning letters stopped sending money overseas for at least a six week period. Rates of detection of those sending money to high risk jurisdictions have also fallen. Both of these indicators strongly suggest that the program is having a substantial impact on reducing the losses arising from relationship scams. Given the success of the program to date, the ACCC proposes to extend the reach of the program in 2015 to include Victoria, Tasmania and the Northern Territory. This will give national coverage to scam disruption projects,

with Queensland, Western Australia and South Australia having similar programs in place that are also achieving good results.

Enforcement

- In April 2014 the ACCC successfully took court action against a company for failing to disclose that its Directors were knowingly involved in making false and misleading statements about the earning potential of franchises. The scam involved the sale of business opportunities to sell weight loss products they claimed were clinically proven. The Court found the clinical trial was a fabrication intended to mislead prospective franchisees and that Peter Foster orchestrated the way in which the business was carried on. Earlier in the year the Federal Court dismissed an appeal by Peter Foster against a three year imprisonment sentence following an ACCC contempt action.

2. Scam contacts and trends

2.1 Scam contact levels

In 2014 the ACCC received 91 637 scam-related contacts (90 561 complaints and 1076 inquiries).

This report is based solely on scam-related contacts to the ACCC and thus provides only part of the picture in terms of the scale of scams activity in Australia. The ACCC is just one of the primary government reporting agencies for scams, with many other authorities also performing an important role in assisting scam victims, including local consumer protection and law enforcement bodies. The Australian Cybercrime Online Reporting Network (ACORN) was also launched in late 2014 and provided a further avenue for the general public to report scams and other fraudulent conduct occurring online. Those targeted by scams may not report at all, particularly where they have not identified or recognised the scam, or where no financial loss has occurred. Further, many scam victims may be too embarrassed to report their experience.

Figure 1 provides a comparison of scam-related contacts to the ACCC over the past six years, which shows an early upward trend with a levelling out in contact levels over the last three years.

Figure 1: Number of scam-related contacts to the ACCC 2009–2014



2.2 Financial losses to scams

In 2014 reports of financial losses arising from scams activity totalled \$81 832 793, representing an 8 per cent decrease on the amount reported in 2013 (\$89 136 975). This is a reverse in trend from 2011 and 2012 where large increases were observed.

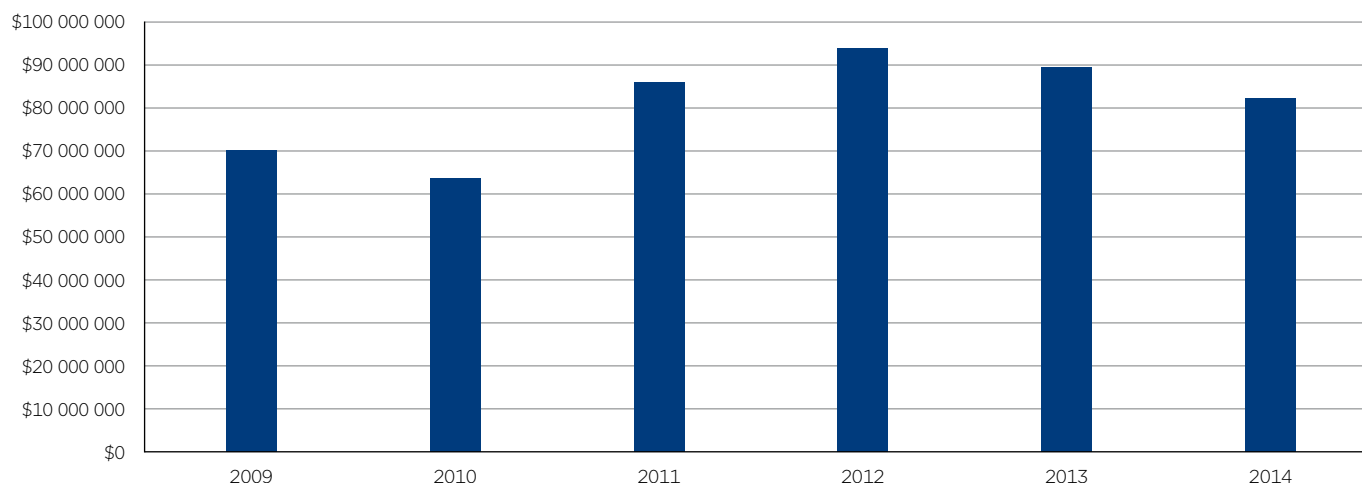
It is important to note that this total is based only on information provided only to the ACCC and as such is likely to represent only a fraction of the financial losses suffered by Australians to scams in 2014.

In 2014 the number of consumers and businesses who contacted the ACCC about scams and who reported no financial loss rose to almost 88 per cent. The remaining 12 per cent reported losses ranging from very small amounts for unsolicited credit card deductions, dubious quality security software and non-receipt of goods bought online to significant losses of \$500 000 or more being reported in respect of investment and dating and romance scams.

The ACCC recognises that some reported losses may represent amounts that people believe they would have been entitled to if the offer were genuine. Where these reports have been identified, the reported loss has been removed from the data.

Figure 2 provides a comparison of scam-related financial losses reported to the ACCC over the past six years, with a slight decrease observed in the last two years.

Figure 2: Reported financial losses to the ACCC from 2009 to 2014



In 2014 the ACCC made changes to the way in which scams were recorded to keep abreast with the evolving nature of scams, gain a clearer picture of the different scam types currently targeting Australians and ensure consistency of data with that collected by other agencies - in particular, ACORN. The changes incorporate a two tier system to assist those reporting to better classify scams. The first tier broadly groups seven scam types into unexpected money, unexpected prizes, threats and extortion, buying and selling, dating and romance, attempts to gain personal information and jobs and investment scams. Each of these categories is then further classified by specific scam types. A glossary of each of the tier 2 scams categories is at appendix 1.

Table 1 provides an overview of financial losses reported against each scam category and sub-category. The top three scam sub-categories in terms of money lost were dating and romance, investment fraud and computer prediction software scams, which are often dressed up as investment opportunities. These three scams account for 60 per cent of reported financial losses.

A list of scam categories by state and territory is provided at appendix 2.

Table 1: Overview of scam types reported to the ACCC in 2014 by Scam Category Level 1

| Scam category level 1 | Scam category level 2 | Amount reported lost | Contacts | Contacts reporting loss | Contacts reporting no loss | Less than \$10k lost | Greater than \$10k lost | Conversion rate |
|--|-------------------------------------|----------------------|---------------|-------------------------|----------------------------|----------------------|-------------------------|-----------------|
| Attempts to gain your personal information (fake bank or telco, computer hacking, ID theft) | Hacking | \$2 252 292 | 4 443 | 328 | 4 115 | 303 | 25 | 7.4% |
| | ID theft involving spam or phishing | \$773 269 | 8 079 | 420 | 7 659 | 401 | 19 | 5.2% |
| | Phishing | \$539 807 | 12 982 | 288 | 12 694 | 278 | 10 | 2.2% |
| | Sub total | \$3 565 368 | 25 504 | 1 036 | 24 468 | 982 | 54 | 4.1% |
| Buying, selling or donating (classifieds, business listings, auction, health, fake business, etc.) | Classified scams | \$1 950 366 | 3 218 | 782 | 2 436 | 732 | 50 | 24.3% |
| | Fake charity scams | \$164 714 | 677 | 107 | 570 | 104 | 3 | 15.8% |
| | Fake trader websites | \$2 134 163 | 2 093 | 1 369 | 724 | 1 326 | 43 | 65.4% |
| | False billing | \$509 605 | 2 652 | 310 | 2 342 | 303 | 7 | 11.7% |
| | Health and medical products | \$71 893 | 403 | 191 | 212 | 191 | 0 | 47.4% |
| | Mobile premium services | \$22 271 | 257 | 98 | 159 | 97 | 1 | 38.1% |
| | Other buying and selling scams | \$3 211 456 | 6 953 | 2 437 | 4 516 | 2 367 | 70 | 35.0% |
| | Overpayment scams | \$1 521 374 | 1 293 | 188 | 1 105 | 175 | 13 | 14.5% |
| | Psychic and clairvoyant | \$495 276 | 46 | 18 | 28 | 16 | 2 | 39.1% |
| | Remote access scams | \$1 170 759 | 8 814 | 762 | 8 052 | 737 | 25 | 8.6% |
| | Sub total | \$11 251 877 | 26 406 | 6 262 | 20 144 | 6 048 | 214 | 23.7% |

| Scam category level 1 | Scam category level 2 | Amount reported lost | Contacts | Contacts reporting loss | Contacts reporting no loss | Less than \$10k lost | Greater than \$10k lost | Conversion rate |
|--|--|----------------------|---------------|-------------------------|----------------------------|----------------------|-------------------------|-----------------|
| Dating and Romance | Dating and romance | \$27 904 562 | 2 497 | 1 032 | 1 465 | 659 | 373 | 41.3% |
| | Sub total | \$27 904 562 | 2 497 | 1 032 | 1 465 | 659 | 373 | 41.3% |
| Jobs and investment (sport, high return, pyramid scheme, employment) | Computer prediction software and sports investment schemes | \$9 039 340 | 487 | 256 | 231 | 117 | 139 | 52.6% |
| | Investment schemes | \$12 462 624 | 938 | 316 | 622 | 121 | 195 | 33.7% |
| | Job and employment | \$938 196 | 1 888 | 256 | 1 632 | 232 | 24 | 13.6% |
| | Other business, employment and investment scams | \$2 481 117 | 954 | 201 | 753 | 160 | 41 | 21.1% |
| | Pyramid schemes | \$217 675 | 229 | 36 | 193 | 31 | 5 | 15.7% |
| | Sub total | \$25 138 952 | 4 496 | 1 065 | 3 431 | 661 | 404 | 23.7% |
| Threats and extortion (ransomware, malware and software, hitman, etc.) | Hitman scams | \$280 228 | 280 | 34 | 246 | 28 | 6 | 12.1% |
| | Ransomware and malware | \$977 044 | 2 556 | 160 | 2 396 | 145 | 15 | 6.3% |
| | Sub total | \$1 257 272 | 2 836 | 194 | 2 642 | 173 | 21 | 6.8% |
| Unexpected money (inheritance, helping a foreigner, fake government or bank, loan opportunity) | Inheritance scams | \$3 888 275 | 4 358 | 89 | 4 269 | 43 | 46 | 2.0% |
| | Nigerian scams | \$2 193 094 | 1 053 | 86 | 967 | 57 | 29 | 8.2% |
| | Other upfront payment and advanced fee frauds | \$3 336 406 | 4 143 | 652 | 3 491 | 598 | 54 | 15.7% |
| | Reclaim scams | \$980 165 | 13 905 | 255 | 13 650 | 240 | 15 | 1.8% |
| | Sub total | \$10 397 940 | 23 459 | 1 082 | 22 377 | 938 | 144 | 4.6% |
| Unexpected Prizes (lottery, travel, scratchie) | Scratchie scams | \$297 593 | 632 | 34 | 598 | 24 | 10 | 5.4% |
| | Travel prize scams | \$107 950 | 1 717 | 83 | 1 634 | 81 | 2 | 4.8% |
| | Unexpected prize and lottery scams | \$1 890 265 | 3 315 | 271 | 3 044 | 243 | 28 | 8.2% |
| | Sub total | \$2 295 808 | 5 664 | 388 | 5 276 | 348 | 40 | 6.9% |
| Not Supplied | Insufficient detail provided to classify scam | \$21 014 | 775 | 27 | 748 | 27 | 0 | 3.5% |
| | Total | \$81 832 793 | 91 637 | 11 086 | 80 551 | 9 836 | 1 250 | 12.1% |

The true cost of scams

The impact of scams on Australian society and the economy is substantial, with financial losses just one part of the picture.

Financial losses

Reports of financial losses to the ACCC are only the tip of the iceberg as scam victims may report to other authorities, may be unwilling to report their experience, or may not even realise they have been scammed.

The Australian Bureau of Statistics' most recent *Personal Fraud Survey* (2010–11) estimates that Australians lost \$1.4 billion to personal fraud (which includes credit card fraud, identity theft and scams).*

The financial repercussions resulting out of scams victimisation can range from a few dollars to losing one's life savings and/or house.

Non-financial losses

Scams can also devastate the lives of victims and their families beyond financial costs, with the emotional toll of these experiences an unquantifiable loss.

Individuals may suffer adverse effects on their mental health, work capacity, relationships and family.

Victims often suffer in silence as they are too embarrassed to speak up about their experience and seek help.

In reality, everyone is vulnerable to scams at some stage in life (see page 30 for more information).

Economic and societal losses

The cost of scams to the Australian economy and society more broadly should not be underestimated, with significant flow-on effects as a result of this activity.

Scams can cause significant harm to businesses through loss of revenue either directly as victims, indirectly through scammers impersonating them, or in costs associated with on-going monitoring and security upgrades.

Scammers also increasingly undermine legitimate corporate and government entities by misusing consumers' trust in well-known brands, reputations and authority.

At the same time, consumer trust in new or evolving products, services and markets is undermined by scams activity, with one bad experience sufficient to discourage future participation in these parts of the economy.

Where scams result in total financial loss, victims ultimately become dependent on Australia's welfare system.

* Australian Bureau of Statistics, *Personal fraud survey 2010–2011*, Canberra, April 2012.

Table 2 provides a comparison of financial losses reported to the ACCC in 2014 and 2013 by loss range. As with previous years, scammers continued to favour sending 'high volume scams', which involve targeting a large number of victims with requests for small amounts of money. Fortunately, there were no reported losses in excess of \$1 million in 2014 but there were still 14 reported losses over \$500 000.

Table 2: Comparison of scam-related monetary losses reported to the ACCC in 2014 and 2013

| Loss categories \$ | 2014 | Percentage 2014 | 2013 | Percentage 2013 | Variance to 2013 |
|----------------------|---------------|-----------------|---------------|-----------------|------------------|
| 1-99 | 1 834 | 16.5% | 1 949 | 15.3% | 1.2 |
| 100-499 | 3 957 | 35.7% | 4 155 | 32.6% | 3.1 |
| 500-999 | 1 469 | 13.3% | 2 096 | 16.5% | -3.2 |
| 1000-9999 | 2 576 | 23.2% | 3 214 | 25.2% | -2.0 |
| 10 000-49 999 | 884 | 8.0% | 961 | 7.5% | 0.5 |
| 50 000-499 999 | 352 | 3.2% | 340 | 2.7% | 0.5 |
| 500 000-999 999 | 14 | 0.1% | 15 | 0.1% | 0.0 |
| 1 million-10 million | 0 | 0% | 2 | 0.02% | -0.02 |
| Total | 11 086 | 100% | 12 732 | 100% | |

2.3 Scam delivery methods

Scammers adopt a range of communication channels to deliver scams, and are quick to change their approach to exploit new developments in technology or popular mediums.

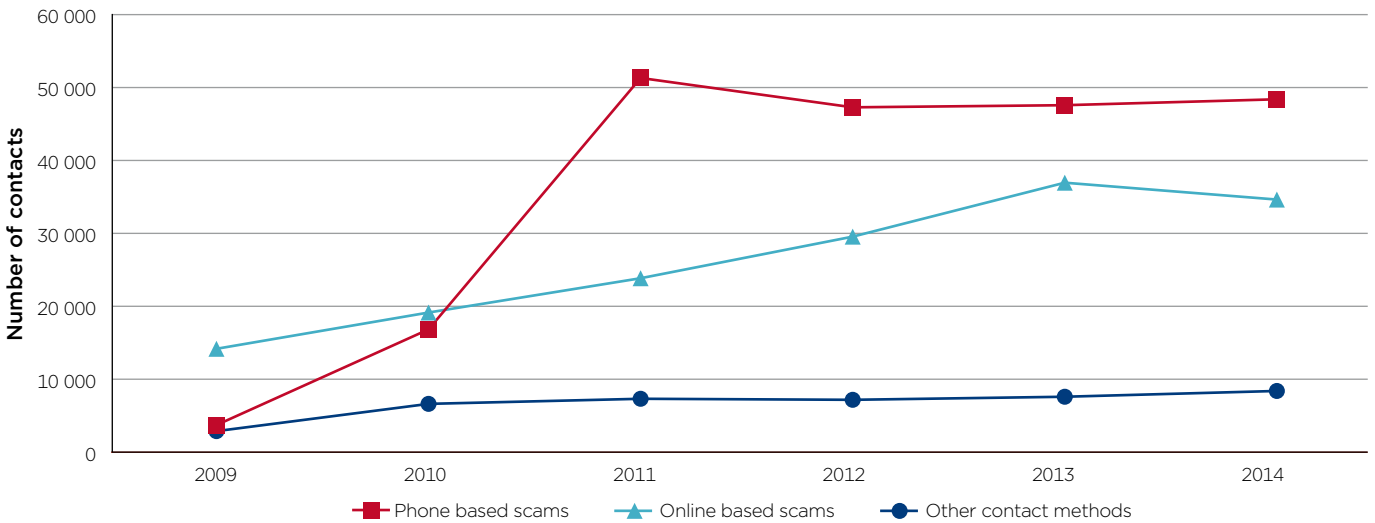
Table 3 provides a comparison of all scam delivery methods reported to the ACCC in 2014 and 2013, highlighting that scams delivered by phone (telephone calls and text messages) continued to be the most common method of targeting the public. Online delivery methods also continued to be favoured by scammers in 2014.

Table 3: Scam delivery methods during 2014 and 2013 based on reports to the ACCC

| Scammer contact mode | 2014 | Percentage | 2013 | Percentage |
|---------------------------------|---------------|-------------|---------------|-------------|
| Phone | 44 411 | 48.5% | 39 916 | 43.4% |
| Text Message | 3 907 | 4.3% | 7 586 | 8.3% |
| Email | 22 858 | 24.9% | 22 155 | 24.1% |
| Internet | 9 108 | 9.9% | 14 695 | 16.0% |
| Social networking/Online forums | 2 367 | 2.6% | 29 | 0.0% |
| Mobile Apps | 233 | 0.3% | 5 | 0.0% |
| Mail | 6 357 | 6.9% | 5 845 | 6.4% |
| In Person | 1 431 | 1.6% | 1 055 | 1.1% |
| Fax | 530 | 0.6% | 625 | 0.7% |
| Not supplied | 435 | 0.5% | 16 | 0.0% |
| Total | 91 637 | 100% | 91 927 | 100% |

Figure 3 provides an overview of scam delivery methods over the past six years.

Figure 3: Scam delivery methods 2009–2014 based on reports to the ACCC



Scams delivered by phone (landline and mobile)

In 2014 phone (landline and mobile) remained the most common scams delivery method reported to the ACCC. Almost 53 per cent of reported scams were delivered in this manner (48 318 contacts), with reported financial losses totalling \$23 470 222.

Telephone calls remained the most popular scam contact method, with reports rising by more than 11 per cent from 2013 to 44 411 but reported financial losses fell by approximately \$6 000 000. This decrease may be related to the inclusion of two new categories for mobile apps and social networking, which are often delivered by phone. Those two new categories combined had reported losses of \$6 461 209.

Scams delivered by text message decreased by 48 per cent from 2013 levels, while reported losses increased 7 per cent to \$1 970 265. This increase can be attributed to nine contacts that reported losses of over \$70 000 and arose from a scam delivered via text message. Each of these matters was an advance fee fraud. However, because scam contact mode is classified on the basis of what is reported by the victim it is not always clear if the scam originated as a text message or if this was the mode of communication adopted by the scammer later in the course of the scam.

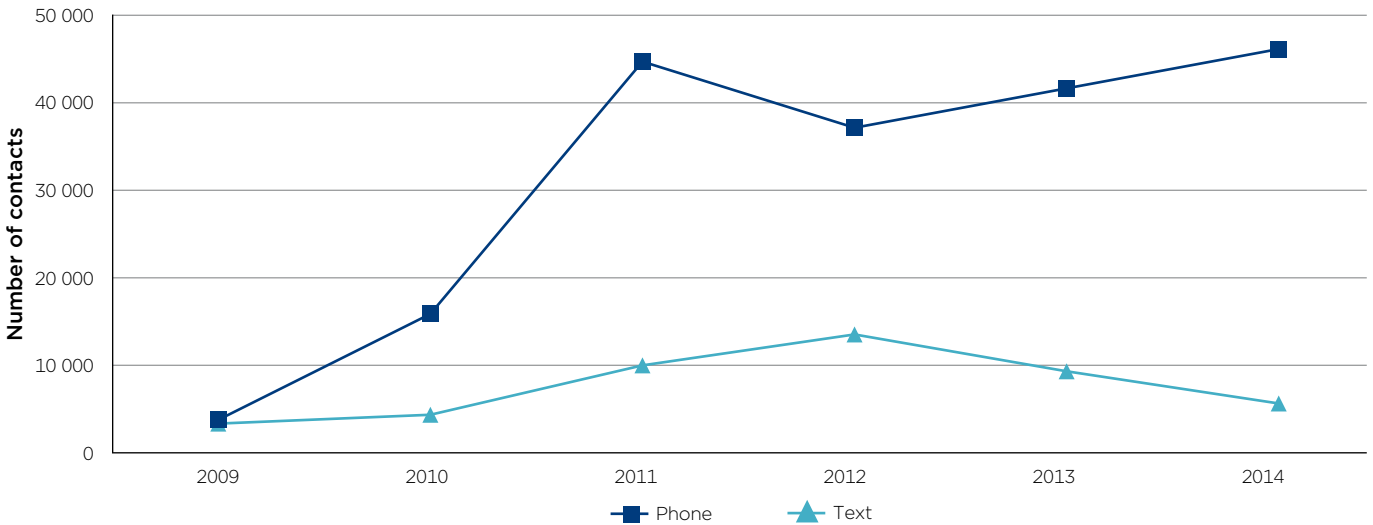
The most prominent scams delivered via telephone calls were reclaim scams, remote access scams and phishing and identity theft scams. The vast majority of scams delivered via text message were unexpected prize and lottery scams, buying and selling scams and phishing.

Scammers typically called or sent text messages where they pretended to be from government or large well-known companies including banks, computer companies, telecommunications service providers and lottery agencies.

As with previous years, the ACCC continued to receive reports that indicate many telephone scams may be operating through overseas call centres. This is likely to be due to the continued use by scammers of cheap scripted call centre operations run by overseas providers, as well as the growing availability of low or no-cost VoIP call services. These cold calling scams are usually directed at the home telephone and account for the majority of telephone scams reported to the ACCC.

Figure 4 highlights the shift in scams delivered via a phone call or SMS reported to the ACCC over the past six years.

Figure 4: Scams delivered via telephone (voice and text message) 2009–14



Scams delivered online (internet and email)

In 2014 scammers continued to take advantage of the online environment to deliver scams to Australians, with this delivery method netting the highest financial losses.

Contacts of scams delivered online decreased in 2014 by 6 per cent to represent just fewer than 38 per cent of all scam approaches. The ACCC received 9108 reports of scams delivered via the internet, 22 858 reports of scams delivered via email, 2367 through social networking sites and 233 from mobile apps. These latter two categories were added in 2014.

Total reported financial losses from online scams increased in 2014 by 13 per cent to \$47 387 308. As noted earlier, this additional \$6 million dollars in losses may be due to a transfer of matters previously classified as originating by phone. With the increased use of smart phone technology, the line between scams originating online or via telephone becomes blurred.

Losses arising out of scams delivered via email increased significantly by 55 per cent to \$19 180 568. This increase contrasts with the significant decrease in 2013 and signals a return closer to those losses to scams via email experienced in 2012. In 2014, dating and romance scams accounted for 30 per cent of these losses. Past experience shows that these scams actually originate from dating sites or through social networking sites but scammers move quickly to get their victims to correspond via phone or email, away from any scrutiny online dating sites might conduct. The discrepancy in figures in the years 2012, 2013 and 2014 could simply be due to the manner in which a few of these high loss scams have been categorised by those that report them.

Online communication channels such as email and social networking forums allow scammers to communicate anonymously from anywhere in the world. The internet provides scammers with a smokescreen to hide behind, with the global and anonymous nature of the online environment helping to mask their physical location.

The increasing availability of wireless internet connectivity and uptake of smart phone technology means that the public needs to be constantly alert to new scam approaches. Scammers will take advantage of the internet to transmit scams to any personal device that is connected to the web—whether it is via the home computer, a smart phone, or anywhere through a tablet.

Misuse of consumer trust and data online

In the online environment, scammers are quick to exploit not only consumer trust, but also data, in their efforts to secure financial gain.

Consumer trust

Misuse of consumer trust online is rife as scammers take advantage of well-known corporations or authorities, or legitimate and popular online communication platforms, to pretend to be genuine.

Online shopping scams are premised on scammers deceiving victims into thinking that they are transacting with a legitimate buyer or seller, with activity often occurring on trusted shopping platforms.

In the classic phishing scam, email platforms are used to deliver scams into people's inboxes that appear to come from a trusted entity such as a financial institution or government body, with the scammer 'phishing' for personal or financial details.

Scammers are also not afraid to adopt a more personalised approach, using social networking forums to 'befriend' victims and then use their personal information against them.

Scammers will create mirror websites where consumers believe that they are transacting with a legitimate company, but instead are being tricked into handing over personal information and money.

The flow on effect of this activity can be significant, with the possibility that consumers will be more likely to stop participating as digital citizens after having been defrauded.

Personal data

Like legitimate businesses, scammers recognise the value of personal data—a commodity that is only going to increase in value with the uptake of online shopping. In the context of scams activity, personal data is a commodity in itself with scammers buying and selling identity kits in black markets to commit other criminal acts.

Scammers harvest personal data online in a number of ways. The phishing scam is the most common approach, with people responding to phoney requests for information that sound plausible at the time. Scammers hack into computers and use malicious software to gain access to personal information stored within. They may also simply listen in on conversations that take place on social networking forums.

Personal data can open the door for a scammer to carry out a range of criminal activity. In some of the more sophisticated scams, personal data is used as the basis of social engineering whereby the target has their own information used against them to manipulate them into falling victim. This is especially common in relationship scams where knowledge of the victim's likes and dislikes are used to build a bond and/or sympathy for the scammer.

When engaging online, it is critical that consumers consider who they are sharing their data with to avoid it being misused.

2.4 Demographics

Demographics are a useful tool in scam prevention by providing authorities with a deeper understanding of where scams are causing the most harm based on personal dimensions such as age, gender and location. This information can help inform what areas of the community are being most affected by scams and thereby inform possible targeted prevention strategies.

New scam demographics

In 2013 the ACCC reviewed its collection of scams data and made several improvements to the way in which information is gathered, including demographics data. Previously the ACCC had a narrower field of demographic data collection covering age and location.

As of January 2014 individuals reporting scams activity to the ACCC have the option to self-identify personal information including, their age, gender, whether they were a small business, or from a disadvantaged or vulnerable background.

This additional data enables the ACCC to better understand where scams are being targeted, or if particular community groups display vulnerabilities that increase their susceptibility to scams.

A snapshot of what the ACCC has identified on scams demographics for 2014 is below and includes a summary of contacts by age, location and gender. Further demographic data is provided for each of the top ten scams in chapter 3.

Age range

The following information is a summary of observations about the age range of people who reported scams activity to the ACCC. The increase in demographic data in 2014 resulted in 41 384 contacts providing age related data compared with only 2152 in 2013.

Table 4 outlines scam contacts to the ACCC where individuals self-identified their age. The data demonstrates that young people were not overrepresented in scam contacts to the ACCC, with people aged under 25 continuing to comprise around 8 per cent of contacts where age range was indicated.

All other age categories were fairly evenly distributed with each category contributing approximately 18 per cent of scam contacts where age was provided.

Table 4 also provides a comparison of scam conversion rates by age range. The conversion rate is the percentage of scam contacts that report a loss. A low conversion rate would indicate a high probability that the scam is recognisable while a high conversion rate suggests that a scam is more likely to result in the loss of money.

In 2014 individuals under 18 years were less likely to report a scam to the ACCC, yet had the highest conversion rate of all groups at 29 per cent. Progressing through the spectrum the conversion rate diminishes to just 11 per cent for those aged 65 and over and suggests reporting the loss of money becomes less important for older age groups.

Table 4: Age ranges provided by consumers reporting scams to the ACCC in 2014

| Age range | No. | % total | Reporting loss | Reporting no loss | Conversion rate |
|--------------|---------------|-------------|----------------|-------------------|-----------------|
| Under 18 | 393 | 1% | 114 | 279 | 29% |
| 18-24 | 3 268 | 8% | 883 | 2 385 | 27% |
| 25-34 | 7 421 | 18% | 1 638 | 5 783 | 22% |
| 35-44 | 7 393 | 18% | 1 326 | 6 067 | 18% |
| 45-54 | 7 989 | 19% | 1 295 | 6 694 | 16% |
| 55-64 | 7 484 | 18% | 993 | 6 491 | 13% |
| 65 and over | 7 436 | 18% | 800 | 6 636 | 11% |
| Total | 41 384 | 100% | 7 049 | 34 335 | 17% |

Geographic location

The ACCC also collects data on the geographic location of people reporting scams.

Figure 5 shows a comparison of scam contacts received by the ACCC in 2014 from within Australia. New South Wales again received the greatest number of scam reports followed by Queensland and Victoria. Contacts for the remaining states and territories were below 10 per cent.

In addition to the above figures the ACCC received 1432 scam contacts from people based overseas, and a further 324 where their location was not provided, representing less than 2 per cent of total contacts.

Figure 5: Scam contacts' location by state and territory 2014

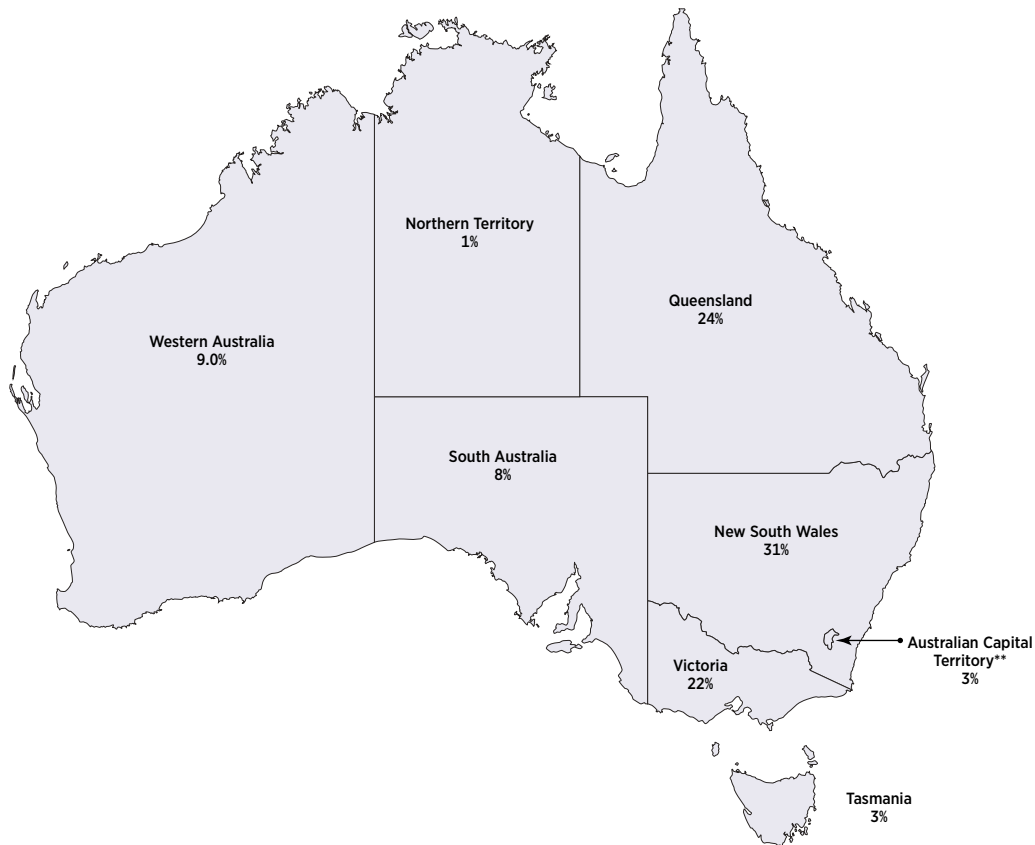


Table 5 provides a comparison of scam contact levels and financial losses against the distribution of the Australian population as a whole. Contact levels and associated losses reported to the ACCC were largely consistent with the percentage of the Australian population by state and territory.

A breakdown of scam categories by state and territory is provided at appendix 2.

Table 5: Scam contacts' location by state and territory 2014

| State | Percentage of total contacts that were based in Australia | Percentage of reported loss where contacts were based in Australia | Percentage of Australian Population* |
|--------------|---|--|--------------------------------------|
| NSW | 31% | 30% | 32% |
| QLD | 24% | 24% | 20% |
| VIC | 22% | 27% | 25% |
| WA | 9% | 10% | 11% |
| SA | 8% | 4% | 7% |
| ACT | 3% | 3% | 2% |
| TAS | 3% | 2% | 2% |
| NT | 1% | 0.5% | 1% |
| Total | 100% | 100% | 100% |

* Australian Bureau of Statistics' Australian Demographic Statistics Jun 2014, released Dec. 2014.

2.5 Conversion rates

Measuring the impact of a scam

Conversion rates show the percentage of people that report a loss resulting from a scam, as opposed to those that recognise a scam and simply report it.

The conversion rate is a useful tool in understanding which scams are more likely to result in consumer harm. Essentially, the conversion rate indicates the 'success rate' of a scam type by revealing how likely it is that an individual who receives and responds to a particular scam will go on to lose money.

Conversely, the lower the conversion rate, the greater the likelihood that more people are successful at recognising a scam and avoiding victimisation.

The overall scam conversion rate decreased from around 14 per cent in 2013 to 12 per cent in 2014.

The relatively low percentage of people reporting a financial loss suggests that the public is generally alert to scams activity and how they can protect themselves. It may also reflect the success of the concerted efforts of the ACCC and many other agencies to raise community awareness so that Australians are better able to identify scams and avoid victimisation.

While it is positive that the conversion rate remains relatively low, there are several factors that make it difficult to grasp a complete picture of the scale and scope of scams activity in Australia.

Scams activity will always be under-reported as recipients may not recognise a scam when they receive it, may not report it where a loss did not arise, or may be too embarrassed to report their experience.

Additionally, there are many other government agencies that play an important role in dealing with scams activity, and to whom consumers can report a scam and seek help. In late 2014 the Australian Cybercrime Online Reporting Network (ACORN) was launched and provides an additional online portal for victims of cybercrime to report matters for possible investigation by police and other authorities. The data collected through ACORN helps to create a fuller picture of the extent of scams that occur online—see section 7.4 for more information.

Some scam categories achieve very high conversion rates and may highlight a particular susceptibility of victims to these types of scams. A high conversion rate is therefore one of the factors that the ACCC considers when deciding where to direct its resources. This is why the ACCC focussed efforts on relationship scams in 2014—see highlight box on page 16—and will continue to do so in 2015.

Table 6 compares conversion rates by scam categories in 2013 and 2014. The change in scam categories means that there is not always corresponding data for all classifications. Figures provided as sub-totals are an approximation of conversion rates based on an amalgamation of new or pre-existing categories and should be considered as indicative only.

The conversion rate for computer prediction software and sports investment schemes saw significant increases, as did investment scams more generally.

The percentage of people reporting losses for health and medical scams decreased and proportionately fewer people reported losses arising from the spread of malicious software (malware).

Table 6: Conversion rates by scam category 2013-14

| Scam Category Level 1 | Scam Category Level 2 | Conversion rate 2014 | Conversion rate 2013 |
|--|--|----------------------|----------------------|
| Attempts to gain your personal information (fake bank or telco, computer hacking, ID theft) | Hacking | 7.4% | |
| | ID theft involving spam or phishing | 5.2% | |
| | Phishing | 2.2% | |
| | Sub total | 4.1% | 4.4% |
| Buying, selling or donating (classifieds, business listings, auction, health, fake business, etc.) | Classified scams | 24.3% | |
| | Fake charity scams | 15.8% | |
| | Fake trader websites | 65.4% | |
| | False billing | 11.7% | 12.1% |
| | Health and medical products | 47.4% | 54.5% |
| | Mobile premium services | 38.1% | |
| | Other buying and selling scams | 35.0% | |
| | Overpayment scams | 14.5% | |
| | Psychic and clairvoyant | 39.1% | 43.9% |
| | Remote access scams | 8.6% | |
| Sub total | 23.7% | | |
| Dating and Romance (including Adult Services) | Dating and romance | 41.3% | 42.8% |
| | Sub total | 41.3% | |
| Jobs and investment (sport, high return, pyramid scheme, employment) | Computer prediction software and sports investment schemes | 52.6% | 37.8% |
| | Investment schemes | 33.7% | 28.3% |
| | Job and employment | 13.6% | 13.5% |
| | Other business, employment and investment scams | 21.1% | |
| | Pyramid schemes | 15.7% | 15.3% |
| Sub total | 23.7% | | |
| Threats and extortion (malware and software by email, malware and software by phone, hitman etc) | Hitman scams | 12.1% | |
| | Ransomware and malware | 6.3% | 9.0% |
| | Sub total | 6.8% | |
| Unexpected money (inheritance, helping a foreigner, fake government or bank, loan opportunity) | Inheritance scams | 2.0% | |
| | Nigerian scams | 8.2% | |
| | Other upfront payment and advanced fee frauds | 15.7% | |
| | Reclaim scams | 1.8% | |
| Sub total | 4.6% | | |
| Unexpected Prizes (lottery, travel, scratchie) | Scratchie scams | 5.4% | |
| | Travel prize scams | 4.8% | |
| | Unexpected prize and lottery scams | 8.2% | |
| Sub total | 6.9% | 5.8% | |
| Not Supplied | | 3.5% | 7.7% |
| Total | | 12.1% | 13.9% |

Spotlight on relationship scams

Relationship scams are acts of fraud that are premised on a scammer establishing a relationship with an individual or business in order to secure their personal details or money. They refer to any scam type where the scammer invests time and effort into convincing the victim that a relationship exists and then manipulates them to secure a personal gain. This 'grooming' is frequently the hallmark of online dating scams, investment scams and psychic and clairvoyant scams.

Scammers have recognised that the time invested in grooming a victim can pay handsome dividends. The significant losses reported by victims and higher than average conversion rates observed in scam categories predicated on a deceptive relationship are a testament to the effectiveness of this technique.

Dating and romance scams are the most destructive form of a relationship scam. In 2014 dating and romance scams netted the highest overall financial losses for any scam type, with almost \$28 million reported lost. While the conversion rate for this type of scam has slowly declined in recent years, it continues to be comparatively higher than other scam categories—in 2014 just over 41 per cent of those who reported an approach by an online admirer went on to lose money. These scams also cause significant emotional harm, with many victims reporting a break down in relationships with friends and family as well as financial ruin.

The psychology of a scam

Scammers have recognised that relationships can prove to be a highly profitable investment and are therefore prepared to spend a considerable amount of time engaging with victims to develop a connection. While some people report scammers making their first request for financial assistance within just a few weeks of connecting with them, other reports show that scammers will wait months before requesting money.

Once the first request and money transfer is made, scammers will continue to make further requests for the lifespan of the relationship which can run for many years. The more a victim invests, the less likely they are to end the deceptive relationship for fear of losing everything. This is true of all relationship scams whether they be based on an emotional or commercial relationship offering high returns. The escalation of commitment results in people making irrational decisions to justify past actions and is sometimes known as the 'sunk cost fallacy'. It is not dissimilar to the addictive behavior of gambling. Often a sense of urgency is created by the scammer which also distracts from rational decision making. Of course the problem is compounded because there is always the promise of reward at the end, be it emotional or financial.

Not all victims are motivated by the lure of the dollar and often those that become embroiled in an online dating scam are more interested in the companionship on offer. The motivation for sending money for many stems from a genuine desire to help a friend in need. Scammers often present their predicament as a short term problem that will be repaid when small hurdles are overcome and they can get access to some source of wealth. Buoyed by the prospects of a longer term relationship and a promise of repayment, the victim finds it easier to be generous.

It is of no consequence to scammers that victims make a significant emotional investment as they become more and more entangled in what they believe to be a genuine relationship. Scammers are adept at emotional manipulation, which causes victims to ignore doubts and is a key reason for the high success rate for scammers obtaining large amounts of money from relationship scams.

How does a relationship scam work?

While relationship scams are by nature a personalised experience, there are a range of elements that underpin them.

- **Personalised approach:** scammers are prepared to do their research on who a person or business is in order to maximise their likelihood of success. Social engineering is a practice employed by sophisticated scammers, whereby personal information about the target is collected and then used against them to elicit a response. Scammers may obtain this information online through social networking forums and, in some of the more sophisticated investment scams, they have been known to purchase lead lists to target likely investors.
- **Emotional manipulation:** scammers are experts at playing on people's emotions to slip under their radar. Scammers will appeal to people's charitable side, make an urgent plea for help, or claim to be in love. These approaches are designed to create a sense of guilt, urgency, anxiety and personal attachment that will push targets to fall for the scheme.
- **'Power of the written word':** we have all heard of this expression which explains the phenomenon of attaching more significance to what we see in writing than what we hear. This is exploited by scammers who often prefer to communicate by text and email and go to great lengths to provide documentary evidence to support their stories. Scammers will take advantage of indirect communication channels to connect with victims in a way that disables the normal cues that people rely on for crosschecking information. Often they will avoid chats online or face-to-face meetings to prevent the victim targets from testing the background and story of the scammer.
- **Blackmail:** modern communication channels allow users to participate in videoconferencing and what seems like a private conversation can easily be recorded. Scammers can and do encourage their victims to engage in risqué behavior and then threaten to share compromising images with friends and family. Don't share photos or engage in webcam of a private nature.

Repeat victimisation

Relationship scams can also result in repeat victimisation, whereby the victim unwittingly falls for the scammer over and over again. In order to continue to extract funds from the victim, the scammer may morph one scam type into another, such as approaching a victim who has fallen for them as part of a dating and romance scam with an investment scam or advance fee fraud.

Scams intervention work carried out by law enforcement agencies in Queensland, South Australia and Western Australia has also highlighted that victims who realise they have been duped and cease contact with the scammer will often then be targeted by a secondary scam. This may include the scammer declaring their love anew, offering to return their money, or even pretending to be an official who is contacting them about the original fraud.

Scammers realise that some victims may be more susceptible to scams and therefore produce lists containing their personal details. The lists are then on-sold to other fraudsters who re-target the victim.

Past and upcoming work to disrupt relationship scams

In recent years the ACCC has prioritised efforts aimed at minimising harm arising out of dating and romance scams, and has observed a continuing decline in the conversion rate—from 48 per cent in 2011 to 41 per cent in 2014. In 2014 the ACCC launched a national disruption project aimed at relationship scams and this will continue throughout 2015. For a detailed overview of this project along with the important work already underway by other agencies to disrupt relationship scams, see section 3.1.

3. Disruption and enforcement activities

Disruption and enforcement activity are both important elements of the ACCC's strategy to tackle scams.

Where appropriate, the ACCC will undertake enforcement activity against scammers to stop the conduct and send a deterrence message to others. However, the increasingly sophisticated, overseas and anonymous nature of scams presents considerable difficulties in identifying and prosecuting the perpetrators behind these schemes. Enforcement action is also not always the most effective way of dealing with scams as it is a costly exercise that happens after the damage is done.

In this context, disruption activity—that is, initiatives aimed at intercepting, interrupting and impeding scams—is a key element in minimising and, in some cases, preventing further harm.

This chapter outlines efforts undertaken by the ACCC and others to deter, discourage and disable scammers targeting Australians.

3.1 Scam disruption activities

The ACCC recognises that disruption activity is one of the primary tools to effectively respond to scams given that many scams operate from a foreign jurisdiction which makes traditional law enforcement complex and costly. Disruption activities provide cost effective alternatives for law enforcement agencies to restrict or even prevent scammers from operating and minimise the harm they may otherwise cause. Such disruption activities often do not require scammers to be specifically identified or located. Instead the focus is on collaborative efforts by government agencies and industry to identify intervention opportunities that might:

- prevent scammers from communicating with their targets
- provide timely warnings to better educate consumers that utilise legitimate services
- interrupt the sending of funds.

In 2014 the ACCC's disruption activities focused on relationship scams with a particular focus on dating and romance scams. Working with other government agencies the ACCC undertook a targeted intervention strategy to warn Australians sending funds offshore that they might be the victim of a scam. The ACCC also opened discussions with representatives from the banking industry to examine options for blocking funds transfers where it can be established that scammers are engaging in fraudulent conduct.

Relationship scams and the ACCC's Scam Disruption Project

In August 2014, the ACCC commenced its Scam Disruption Project which aims to stop potential scam victims from sending more money to scammers. The project involves the use of financial intelligence to identify Australians sending funds to West African nations, who are then advised they may have been targeted by a scam. Recipients of the letters are encouraged to contact the ACCC to discuss their situation on a confidential basis.

The project commenced because losses reported for relationship scams continues to be a significant concern with total losses for dating and romance scams in 2014 almost reaching \$28 million. Relationship scams are acts of fraud that are premised on the scammer building a deceptive connection with an individual or business in order to secure their personal details or money.

The project's focus is initially on residents sending money from New South Wales (NSW) and the Australian Capital Territory (ACT). In 2015 the project will expand to also cover Victoria, Tasmania and Northern Territory. (Western Australia, South Australia and Queensland are being covered by local Fair Trading and Police agencies.)

In the five months to the end of December 2014, just over 2000 letters were sent to potential scam victims in NSW and the ACT.

Of those that contacted the ACCC following receipt of a letter and were identified as victims, 75 per cent were involved in dating and romance scams. Just over one third of these people were contacted by the scammer through social media channels. Scammers also target dating websites, email and regular mail, but this year is the first time the ACCC has collected data from scam victims that clearly identifies social media is being used to facilitate fraudulent activity.

The scams were equally targeting men and women but men lost slightly more money than women and accounted for 57 per cent of the losses. Estimated losses from 77 identified victims were over \$2.3 million at an average of almost \$30 000 each. However, estimated losses from all of those identified as sending money to high risk jurisdictions exceeded \$19 million.

Early results show that 70 per cent of those receiving the ACCC's warning letters stopped sending money overseas for at least a six week period. Rates of detection of those sending money to high risk jurisdictions have also fallen. Both of these indicators are improving and strongly suggest that the program is having a positive impact on stemming the flow of funds to scammers.

The project is a joint initiative with the *Australasian Consumer Fraud Taskforce (ACFT)*, including state and territory police and consumer affairs agencies. Given the success of the program to date, the ACCC proposes to extend the reach of the program in 2015 to include Victoria, Tasmania and the Northern Territory.

Case study: Queensland, West Australian, South Australian authorities help scam victims

Other government authorities have also adopted a proactive approach to disrupting scams and protecting local citizens. In particular, authorities in Queensland, Western Australia (WA) and South Australia (SA) have implemented measures to intervene and cease further financial losses from scam victims.

Queensland scams disruption

The Queensland Police Service's Fraud and Corporate Crime Group has led the way in Australia in tackling scams head on, with scam victim intervention a long-standing priority area of their work.

The analysis of financial intelligence data is the primary means by which the Queensland Police Service identifies possible scam victims. This is then followed by victim intervention, which can range from a phone call through to intercepting victims about to board a plane to meet the scammer overseas.

In 2010 the Queensland Police Service set up Australia's first ever scam victims support group, whereby victims work through their experiences in a supportive environment. The Victims of Fraud Support Group meets once a month and is open to any victim of fraud, friend or family member in need of support.

South Australian scams disruption

In May 2013, a dedicated operation named 'Disrepair' was launched to help reduce the flow of cash from South Australian (SA) scam victims. Figures released by SA Police in July 2014 show that funds transfers to known high risk jurisdictions were down by 42 per cent on figures for the corresponding period the previous year.

As part of operation 'Disrepair', Police officers follow the money trail of transfers to West Africa—particularly to the global scam hotspots of Nigeria and Ghana—and identify South Australians who may be sending money without good cause. Police then send a letter to those identified, alerting them to the fact they may be sending money to scammers and in some cases follow up with a home visit or phone call.

West Australian scams disruption

In 2013 the WA Police Major Fraud Squad and the WA Department of Commerce (Consumer Protection) initiated a joint disruption project, 'Project Sunbird', to identify and prevent consumer fraud originating from specific West African countries against WA citizens.

After identifying potential scam victims through financial intelligence data, WA Police and the Department of Commerce approach victims. In the first instance, victims are sent a letter advising that they had been identified as a potential victim of fraud and to cease contact with the scammer and stop sending any further funds overseas. Where financial intelligence reveals that the victim is continuing to send money, a further more specific and targeted letter is sent and then followed up with face-to-face engagement where significant detriment continues.

In 2014, Western Australian victims of romance fraud reported losing a total of \$10 893 901. In addition to reported losses there are believed to be many more victims not identified.²

More than 2000 letters have been sent out since 2013 and every month more are sent. The first letter addressed to the Householder leads to about six of out 10 victims ceasing to send money. Those who continue sending receive a second personalized letter and of that group about 40 per cent stop sending funds.³

While many are unaware that they are being defrauded, others have suspicions and the letters can be an important step in helping them to recognize and confirm they are a victim of fraud.

WA Police and the Department of Commerce also help scam victims access support services to overcome their experience. Further information about Project Sunbird can be found at: http://www.scamnet.wa.gov.au/scamnet/Fight_Back-Project_Sunbird.htm.

Continuing efforts to work with the online dating industry

In 2011–12 the ACCC prioritised compliance work aimed at dating and romance scams after observing significant financial losses by victims of these scams. This trend continues in 2014 and reported losses to this type of scam still highlight a significant problem indicating a particular vulnerability of consumers to these types of scams.

The ACCC released Best Practice Guidelines for the Dating Industry in 2012 following collaboration with dating website operators to identify disruption measures to improve responses to these scams. The guidelines aim to help dating website operators respond to scams targeting their users and they cover three key areas:

- the inclusion of appropriate scam warnings and information on websites
- establishing vetting and checking systems to detect and deal with scammers
- making available to consumers a scam complaint handling mechanism.

In 2014 the ACCC joined an international initiative to protect vulnerable consumers by sweeping dating websites to determine the extent to which the Best Practice Guidelines had been adopted and examine compliance with other Australian Consumer Law provisions. The subsequent report on results of that internet sweep will be used as the basis for a review of the Best Practice Guidelines to be undertaken in 2015.

A high level overview of the findings from the internet sweep is at figure 6. Key areas for improvement include:

- better upfront disclosure of fees, especially by those sites that advertise themselves as free
- simpler contract cancellation—if you can sign up online you should also be able to cancel online
- safeguards for customer information requiring express consent before re-using personal information.

The complete findings and a copy of the report can be found at: <http://www.accc.gov.au/publications/online-dating-industry-report>.

2 WA Department of Commerce media release: http://www.scamnet.wa.gov.au/scamnet/About_WA_ScamNet-Media_and_events-Western_Australians_lose_109_million_to_heartless_romance_scammers.htm

3 Ibid.

Figure 6: Overview of findings from the 2014 sweep of online dating sites



Disruption—don't let scams affect the bottom line of your business

As we adapt to the digital world so do the scammers who utilise all the same services to communicate, connect and transact. Online dating websites, email and telecommunications services, social networking platforms, money transmission and payment services—all of these are essential elements in enabling scammers to perpetrate their fraud.

The ACCC recognises the important role that intermediary businesses have to play in disrupting scams, many of whom have realised that it makes good business sense to invest in fraud prevention systems. Scam activity creates a burden by:

- tying up resources through the misuse of email and other communication services;
- fraudulently using credit and payment facilities and increasing the costs for everyone, and
- undermining the credibility of legitimate businesses.

If a service becomes known as a hot bed for fraudulent activity, it will damage consumer confidence and in the longer term impact negatively on business operations and the bottom line.

Following on from the ACCC's work with the online dating industry and the release of Best Practice Guidelines, feedback was that clients using dating services responded positively and felt more secure dealing with a business that took steps to improve their fraud prevention systems and provide scam prevention messaging.

Other industries have taken similar steps and established systems to detect and prevent scam activity. Scammers will always adapt and will move to those platforms or mediums where their activities might go undetected. Ultimately, those intermediary businesses that don't have systems in place to protect their customers will wear the burden of scammers exploiting their services and risk alienating their customers.

Put simply, fraud prevention makes good business sense.

3.2 Scam-related enforcement activities

ACCC enforcement activity

Where appropriate the ACCC will undertake enforcement action against the perpetrators of scams, particularly where it is likely to have the potential to deter others who may be considering engaging in unscrupulous conduct.

Federal Court finds Sensaslim misled franchisees about Peter Foster's involvement

The Federal Court has found SensaSlim Australia Pty Ltd engaged in misleading or deceptive conduct by failing to disclose Peter Foster's involvement in the SensaSlim franchise system.

The Court also found that SensaSlim engaged in misleading or deceptive conduct by making false representations about the role of a number of SensaSlim's officers who were found to be knowingly concerned in and party to some of SensaSlim's contraventions.

The Courts findings in 2014 arose from the long standing pursuit of those behind a scam to mislead people into purchasing franchises for weight loss products. SensaSlim Australia Pty Ltd supplied an oral spray that was claimed to cause weight loss, and represented that the solution was the subject of 'a large worldwide clinical trial'. The spray was distributed through franchisees to be on-sold to consumers through retail outlets. Around 110 areas were sold to franchisees for the cost of \$59 950 each. SensaSlim earned approximately \$6.4 million from the sale of these franchises.

In his judgment, Justice Yates found that, 'the evidence presents a convincing picture of Mr Foster as the puppeteer who pulled all the strings [in SensaSlim]' and 'Mr Foster controlled and directed, in an executive capacity, the way in which the SensaSlim business was carried on.' He said that 'the failure to disclose Mr Foster in the Disclosure Document was deliberate.'

His Honour also found that 'the clinical study of the SensaSlim Solution ... is a fabrication, intended to lead prospective franchisees into the false belief that the efficacy of the SensaSlim product as weight loss product had been established scientifically'.

This case was particularly significant because Mr Foster went to great lengths in order to hide his involvement in the SensaSlim business from franchisees and others.

In a separate but related decision, the Federal Court dismissed an appeal by Mr Foster against his three year imprisonment sentence that arose out of earlier contempt proceedings for breach of court orders. Mr Foster filed this appeal without personally appearing before the Court, at a time when he had failed to surrender himself to the court and there were outstanding warrants for his arrest and imprisonment.

Justice Dowsett found that Mr Foster has blatantly disregarded the court order of 26 September 2013, requiring his court attendance on 27 September 2013. Mr Foster did not offer any justification for not attending court. In October 2014 Mr Foster was arrested for failing to appear at a sentencing hearing.

The cases demonstrate that the ACCC will take all necessary action to ensure that court orders designed to protect consumers are enforced.

4. The top 10: 2014's most significant scams

4.1 Overview of most common scam types reported to the ACCC

In 2014 the ACCC continued receiving contacts about a broad range of scams targeting Australians.

Table 7 provides an overview of all scam types reported to the ACCC in 2014 in order of number of contacts per category.

A list of scam categories by state and territory is provided at appendix 2.

Table 7: Overview of scam types reported to the ACCC in 2014 in order of contact levels

| Scam category | Amount reported lost | Contacts | Contacts reporting no loss | Contacts reporting loss | Less than \$10k lost | Greater than \$10k and less than \$100k lost | Greater than \$100k lost | Conversion rate |
|--|----------------------|--------------|----------------------------|-------------------------|----------------------|--|--------------------------|-----------------|
| Reclaim scams | \$980 165 | 13905 | 13650 | 255 | 240 | 14 | 1 | 1.8% |
| Phishing | \$539 807 | 12982 | 12694 | 288 | 278 | 10 | | 2.2% |
| Remote access scams | \$1 170 759 | 8814 | 8052 | 762 | 737 | 25 | | 8.6% |
| ID theft involving spam or phishing | \$773 269 | 8079 | 7659 | 420 | 401 | 19 | | 5.2% |
| Other buying and selling scams | \$3 211 456 | 6953 | 4516 | 2437 | 2367 | 70 | | 35.0% |
| Hacking | \$2 252 292 | 4443 | 4115 | 328 | 303 | 20 | 5 | 7.4% |
| Inheritance scams | \$3 888 275 | 4358 | 4269 | 89 | 43 | 36 | 10 | 2.0% |
| Other upfront payment and advanced fee frauds | \$3 336 406 | 4143 | 3491 | 652 | 598 | 50 | 4 | 15.7% |
| Unexpected prize and lottery scams | \$1 890 265 | 3315 | 3044 | 271 | 243 | 21 | 7 | 8.2% |
| Classified scams | \$1 950 366 | 3218 | 2436 | 782 | 732 | 49 | 1 | 24.3% |
| False billing | \$509 605 | 2652 | 2342 | 310 | 303 | 6 | 1 | 11.7% |
| Ransomware and malware | \$977 044 | 2556 | 2396 | 160 | 145 | 11 | 4 | 6.3% |
| Dating and romance | \$27 904 562 | 2497 | 1465 | 1032 | 659 | 292 | 81 | 41.3% |
| Fake trader websites | \$2 134 163 | 2093 | 724 | 1369 | 1326 | 39 | 4 | 65.4% |
| Job and employment | \$938 196 | 1888 | 1632 | 256 | 232 | 23 | 1 | 13.6% |
| Travel prize scams | \$107 950 | 1717 | 1634 | 83 | 81 | 2 | | 4.8% |
| Overpayment scams | \$1 521 374 | 1293 | 1105 | 188 | 175 | 11 | 2 | 14.5% |
| Nigerian scams | \$2 193 094 | 1053 | 967 | 86 | 57 | 23 | 6 | 8.2% |
| Other business, employment and investment scams | \$2 481 117 | 954 | 753 | 201 | 160 | 35 | 6 | 21.1% |
| Investment schemes | \$12 462 624 | 938 | 622 | 316 | 121 | 151 | 44 | 33.7% |
| (blank) | \$21 014 | 775 | 748 | 27 | 27 | | | 3.5% |
| Fake charity scams | \$164 714 | 677 | 570 | 107 | 104 | 3 | | 15.8% |
| Scratchie scams | \$297 593 | 632 | 598 | 34 | 24 | 10 | | 5.4% |
| Computer prediction software and sports investment schemes | \$9 039 340 | 487 | 231 | 256 | 117 | 114 | 25 | 52.6% |
| Health and medical products | \$71 893 | 403 | 212 | 191 | 191 | | | 47.4% |
| Hitman scams | \$280 228 | 280 | 246 | 34 | 28 | 6 | | 12.1% |
| Mobile premium services | \$22 271 | 257 | 159 | 98 | 97 | 1 | | 38.1% |
| Pyramid schemes | \$217 675 | 229 | 193 | 36 | 31 | 4 | 1 | 15.7% |
| Psychic and clairvoyant | \$495 276 | 46 | 28 | 18 | 16 | 1 | 1 | 39.1% |
| Total | \$81 832 793 | 91637 | 80551 | 11086 | 9836 | 1046 | 204 | 12.1% |

4.2 The top 10 scams in 2014 (\$ reported loss)

In 2014 the top scams reported to the ACCC in terms of reported loss continued to be variations of advance fee fraud scams where high returns, untold wealth or love is promised and funds are requested for payment of fake fees and charges.

Table 8 shows the top 10 scam categories* by reported loss for 2014 and provides a comparison of the losses with 2013 where this information is available. Due to changes in scam classification it is not possible to provide comparative losses for all scam categories. Dating and romance scams remained the number one scam for 2014 with an increase of over \$2.5 million in the amount lost to nearly \$28 million. Australians looking to get high returns on investments also suffered significant losses to scams with combined losses of over \$21.5 million. The total losses for investment scams are likely to be significantly higher as many people report these to the Australian Securities and Investment Commission (ASIC). ASIC has a very important role in consumer protection for financial services and maintains the Moneysmart.gov.au website. This site allows people to report investment scams and has excellent resources for people wishing to invest and avoid scams.

Table 8 shows an overview of scams reported to the ACCC in order of reported losses.

Table 8: Overview of scam types reported to the ACCC in 2014 in order of reported loss

| Scam category | Amount reported lost | Contacts | Contacts reporting no loss | Contacts reporting loss | Less than \$10k lost | Greater than \$10k and less than \$100k lost | Greater than \$100k lost | Conversion rate |
|--|----------------------|----------|----------------------------|-------------------------|----------------------|--|--------------------------|-----------------|
| Dating and romance | \$27 904 562 | 2 497 | 1 465 | 1 032 | 659 | 292 | 81 | 41.3% |
| Investment schemes | \$12 462 624 | 938 | 622 | 316 | 121 | 151 | 44 | 33.7% |
| Computer prediction software and sports investment schemes | \$9 039 340 | 487 | 231 | 256 | 117 | 114 | 25 | 52.6% |
| Inheritance scams | \$3 888 275 | 4 358 | 4 269 | 89 | 43 | 36 | 10 | 2.0% |
| Other upfront payment and advanced fee frauds | \$3 336 406 | 4 143 | 3491 | 652 | 598 | 50 | 4 | 15.7% |
| Other buying and selling scams | \$3 211 456 | 6 953 | 4 516 | 2 437 | 2 367 | 70 | | 35.0% |
| Other business, employment and investment scams | \$2 481 117 | 954 | 753 | 201 | 160 | 35 | 6 | 21.1% |
| Hacking | \$2 252 292 | 4 443 | 4 115 | 328 | 303 | 20 | 5 | 7.4% |
| Nigerian scams | \$2 193 094 | 1 053 | 967 | 86 | 57 | 23 | 6 | 8.2% |
| Fake trader websites | \$2 134 163 | 2 093 | 724 | 1 369 | 1 326 | 39 | 4 | 65.4% |
| Classified scams | \$1 950 366 | 3218 | 2436 | 782 | 732 | 49 | 1 | 24.3% |
| Unexpected prize and lottery scams | \$1 890 265 | 3 315 | 3 044 | 271 | 243 | 21 | 7 | 8.2% |
| Overpayment scams | \$1 521 374 | 1 293 | 1 105 | 188 | 175 | 11 | 2 | 14.5% |
| Remote access scams | \$1 170 759 | 8 814 | 8 052 | 762 | 737 | 25 | | 8.6% |
| Reclaim scams | \$980 165 | 13 905 | 13 650 | 255 | 240 | 14 | 1 | 1.8% |
| Ransomware and malware | \$977 044 | 2 556 | 2 396 | 160 | 145 | 11 | 4 | 6.3% |
| Job and employment | \$938 196 | 1 888 | 1 632 | 256 | 232 | 23 | 1 | 13.6% |
| ID theft involving spam or phishing | \$773 269 | 8 079 | 7 659 | 420 | 401 | 19 | | 5.2% |
| Phishing | \$539 807 | 12 982 | 12 694 | 288 | 278 | 10 | | 2.2% |
| False billing | \$509 605 | 2 652 | 2 342 | 310 | 303 | 6 | 1 | 11.7% |
| Psychic and clairvoyant | \$495 276 | 46 | 28 | 18 | 16 | 1 | 1 | 39.1% |
| Scratchie scams | \$297 593 | 632 | 598 | 34 | 24 | 10 | | 5.4% |
| Hitman scams | \$280 228 | 280 | 246 | 34 | 28 | 6 | | 12.1% |
| Pyramid schemes | \$217 675 | 229 | 193 | 36 | 31 | 4 | 1 | 15.7% |

| Scam category | Amount reported lost | Contacts | Contacts reporting no loss | Contacts reporting loss | Less than \$10k lost | Greater than \$10k and less than \$100k lost | Greater than \$100k lost | Conversion rate |
|-----------------------------|----------------------|---------------|----------------------------|-------------------------|----------------------|--|--------------------------|-----------------|
| Fake charity scams | \$164 714 | 677 | 570 | 107 | 104 | 3 | | 15.8% |
| Travel prize scams | \$107 950 | 1 717 | 1 634 | 83 | 81 | 2 | | 4.8% |
| Health and medical products | \$71 893 | 403 | 212 | 191 | 191 | | | 47.4% |
| Mobile premium services | \$22 271 | 257 | 159 | 98 | 97 | 1 | | 38.1% |
| (blank) | \$21 014 | 775 | 748 | 27 | 27 | | | 3.5% |
| Total | \$81 832 793 | 91 637 | 80 551 | 11 086 | 9 836 | 1 046 | 204 | 12.1% |

Table 9: Comparison of the top 10 scam report levels 2013-14

| Top 10 scams by reported loss | 2014 | 2013 |
|--|--------------------|--------------|
| Dating and romance | \$27 904 562 | \$25 247 418 |
| Investment schemes | \$12 462 624 | \$9 083 512 |
| Computer prediction software and sports investment schemes | \$9 039 340 | \$9 144 288 |
| Inheritance scams | \$3 888 275 | |
| Hacking | \$2 252 292 | \$1 130 947 |
| Nigerian scams | \$2 193 094 | |
| Fake trader websites | \$2 134 163 | |
| Classified scams | \$1 950 366 | |
| Unexpected prize and lottery scams | \$1 890 265 | \$995 288 |
| Overpayment scams | \$1 521 374 | |

* The Top 10 scam categories exclude three 'Other' scam categories as these contain a range of scams not easily classified under generic headings.

The following sections summarise the top 10 scams by monetary loss, and include victim stories which are drawn from real life examples of scams reported to the ACCC. Names and details have been changed.

#1. Dating and romance scams

Number of scam reports:
2497

Per cent of total reported loss:
34%

Per cent of total scams reported:
3%

Number of consumers reporting losses:
1032

Total losses reported by consumers:
\$27 904 562

Scam conversion rate:
41%

Most affected age group:
45-64 y.o. 49%

Gender:
Female: 53%
Male: 47%

In 2014 dating and romance scams remained in the number one position in terms of financial losses, with \$27 904 562 reported lost—an increase of more than 10 per cent. The ACCC received 2497 reports of dating and romance scams in 2014, down 10 per cent from the previous year. Financial losses continue to remain substantially disproportionate to contacts, with dating and romance scams making up only 3 per cent of all scam-related contacts.

For the fourth consecutive year the ACCC has observed a decrease in the percentage of people who responded to an approach by a scam admirer and subsequently lost money—this conversion rate fell from 48 per cent in 2011 to 41 per cent in 2014. While it is encouraging that more people are recognising these scams and avoiding losing money, the percentage of those reporting losses is still very high compared to other scam categories. This indicates the effectiveness of a scam that has at its basis the exploitation of a relationship that can be carried out over a long time—in some instances years.

Dating and romance scams start with the victim meeting someone online. The scammers say they come from a western country and claim to be posted overseas overseeing an infrastructure project, working for an oil company or deployed as a soldier or peacekeeping force. The scammer quickly declares his or her love for the victim and the requests for money soon follow.

Excuses for why the victim needs to send money are elaborate and varied but there is always some barrier or event that stops the scammer being able to come to Australia to be with the victim. Victims believe they are helping pay for airline tickets, military leave passes, visa applications, medical expenses or government fees. The requests are endless, promises are never kept and there is always another excuse for why more money is needed.

Scammers often approach their victims on legitimate dating websites before quickly attempting to move the victim away from the security of the site, communicating through other methods such as email. 34 per cent of reports identify the internet as the scammer contact method with 21 per cent by email.

Scammers are also targeting victims through social networking sites, where they 'like' them and then express shared interests based on personal information gleaned from their profile. Almost 30 per cent of dating scams reported meeting through social networking sites or online forums. Clearly, scammers will adapt their approach and follow individuals onto any communication platform—in short, scammers will take advantage of any way to connect with people.

In 2014 the average reported loss from a dating and romance scam was over \$27 000, with around one third of victims reporting losses over \$10 000. With such a high return, it is not surprising that scammers are prepared to invest the time and energy into building a romantic connection.

The ACCC made the disruption of relationship scams a priority of focus area in 2014. Find out more about these scams, and what the ACCC is doing to disrupt them at section 3.1.

Victim's story:

Georgina's Facebook fiancé leaves her flat broke

Georgina's children signed her up to Facebook and gave her some basic lessons on how to use the 'app'.

'They told me everyone was using it and that it would help us keep in touch. They showed me how I could see pictures of my grandchildren and I thought it was marvellous technology.'

Not long after, Georgina received a friend request from a serviceman on peacekeeping duties in Afghanistan. It didn't start as a romance but he said he was lonely and looking for friends to keep him company while he was stuck on duty in the middle of nowhere. Soon after befriending her, Jim told Georgina he had lost his wife to cancer and his story of looking after her was similar to her own experience when her husband had died of cancer.

'He then said he was being posted to Nigeria but his time in the U.S Army was nearly finished. He sent me pictures which I now know were stolen from the internet. He kept saying he couldn't wait for us to be together. We became very close and he emailed me every day saying it was easier for him than using Facebook.'

The scammer told Georgina he liked gemstones and wanted to set up a little jewellery store when he retired. He said this was the best part of being in Nigeria because it was in Africa close to where the precious stones were being mined and he could buy them very cheaply.

He told Georgina he was coming to see her but had some trouble with his bank card not working in Nigeria and couldn't get funds to pay for an export tax on his gemstones. Georgina transferred some money to him to cover the tax which was only two per cent of the value of the gemstones but still amounted to \$15 000. It was a lot of money to send but she figured he was a good and honest serviceman and if things worked out they would spend the rest of their lives together.

'All was proceeding well until his stopover in Malaysia. Customs officials seized the gemstones and demanded payment to have them released. This time they were asking \$20 000. I told him it would take some time to get the money and I had to borrow against the family home.'

Georgina sent the money to Malaysian officials but was told Jim was now in gaol for smuggling and that she needed to contact his lawyer.

'The lawyer said he needed to get an Anti-terrorism and Money Laundering certificate and this would be another \$10 000. He said he also needed to pay for Jim's court costs plus his own fees and this would be another \$5000.'

Georgina sent the money but then there was another government official looking for money to extend Jim's visa while he waited for the court to process all the documents.

'Almost every day I was contacted with a new demand for money. They sent me certificates signed by officials, forms to fill out and bills for everything. If you wanted to get anything done quickly you had to pay another fee. It seemed to me that the whole Malaysian government was corrupt. I don't know exactly how much money I sent but it was well over \$100 000. I didn't care about the money. I just wanted to help Jim and I honestly thought he would pay me back.'

Even when Georgina ran out of money the demands didn't stop. Unsure of what to do, Georgina finally talked to the police who explained the scam. She can't help feeling in her heart that she let Jim down but she knows in her head it was all a scam.

"If you've only ever met online, you need to take extra precautions to protect yourself. Don't let a scammer take advantage of your better nature and steal your money—cease contact with an online admirer if they ask you for financial help, no matter how genuine they sound."

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Be very careful about how much personal information you share on social network sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.
2. Do a 'Google Image' search of your admirer to help tell if they really are who they say they are.
3. Be alert to things like spelling and grammar mistakes, inconsistencies in their stories and other signs that it's a scam like multiple excuses for why they need your money.
4. Think twice: never send money to someone you've met online, especially via money order, wire transfer or international funds transfer—it's almost impossible to recover money sent this way.
5. Never share photos or videos of a personal nature. Scammers will use them to blackmail you once you stop sending them money.

SCAMwatch radar: Don't get scammed into a broken heart and empty wallet



In February 2014 the ACCC issued a SCAMwatch radar warning those looking for a romantic connection online to beware of scammers seeking to steal their heart and money.

Reports to the ACCC showed that scammers continued to target the lonely hearted online, using fake profiles on legitimate dating websites, online forums and through social networking sites. Once trust is gained, the scammer would quickly attempt to move the victim away from the site and its security to communicate and manipulate them into handing over money.

The ACCC also warned that scammers were blackmailing victims by threatening to send potentially compromising photos or videos to their family and friends. Scammers would capture photos or videos from webcam chats, access information from the victim's social network profile and threaten to publically post the compromising images.

Read more at www.scamwatch.gov.au.

Everyone is vulnerable at some stage to a scam

Many people may look at an online dating scam and wonder, 'how could someone fall for this?'

It is important to understand that there are a number of reasons why people fall victim to a scam, and that everyone can be vulnerable at some point in life to a scam approach.

Some vulnerability factors include:

- Personal circumstances—people are more likely to fall for a scam if the ruse personally relates to them, particularly where it elicits an emotional response.
- Charitable nature—some people are more predisposed to want to help those in need, which makes them vulnerable to the many scams that are masked as pleas for help. For example, someone who has lost a loved one to an illness may be more vulnerable to scammers making pleas for financial help to cover costs associated with a medical emergency.
- Urgency—people may respond to a scam when it creates a sense of urgency around something important. Often scammers will create fictitious situations such as having been detained in a foreign jurisdiction and need immediate help with legal expenses or they will claim that a fee needs to be paid within 48 hours to release funds before the government confiscates them.
- Other scams prey on different vulnerabilities. A small business that has unsophisticated accounting systems may inadvertently pay a fraudulent invoice. Someone being offered a phony tax rebate may think this is timely because of mounting bill pressures. Some people just have a 'nothing ventured, nothing gained' attitude to life.
- Many of us find ourselves in a position when personal circumstances make us more vulnerable including:
 - Time-poor—when a person or business is pressured in terms of available time, they may respond to a scam before realising what it is.
 - Financial troubles—when people are experiencing financial difficulties, they may be more likely to ignore cues that an offer is a scam.
 - Gambling or risk-taking personality—some personality types are more likely to accept an offer and see where it will take them, before realising that it is a scam.

It is not only the gullible and greedy that fall victim to a scam and many professional and well educated people have been taken in. Scammers are particularly good at presenting themselves in a convincing light and will use any information they can get to convince their victims to part with their money. The more detail they have about your personal circumstances, the greater the risk of becoming a victim.

By raising awareness of scams and the importance of keeping your personal details secure, the ACCC hopes to alert people to the pitfalls and target-harden the Australian community against fraud.

#2. Investment scams

Number of scam reports:

938

Per cent of total reported loss:

15%

Per cent of total scams reported:

1%

Number of consumers reporting losses:

316

Total losses reported by consumers:

\$12 462 624

Scam conversion rate:

34%

Most affected age group:

25-54 y.o. 69%

Gender:

Female: 34%

Male: 66%

In 2014 the ACCC received 938 reports about investment scams with 316 reporting losses, an increase of 34 per cent from 2013 levels. Financial losses saw a 37 per cent increase from \$9 083 512 in 2013 to \$12 462 624 in 2014.

The percentage of those reporting losses (34 per cent) suggests that many people are unable to distinguish legitimate investment opportunities from outright scams. This is not surprising given the level of sophistication that scammers employ to perpetrate their fraud. With high value gains to be made, scammers can afford to invest heavily in props and scripts to trap the unsuspecting.

Past investigations into this type of fraud found teams of scammers had set up boiler rooms to cold call would-be investors. The scammers even did their homework and purchased lead lists from legitimate marketing companies. They employed people with inside knowledge of the investment industry and had carefully scripted calls to convince their targets of the legitimacy of their operations. Typically operating offshore, they would entice their victims with attractive offers above market rates but would avoid making outlandish offers that would immediately raise suspicions.

The Australian Crime Commission refers to this type of fraud as serious and organised investment fraud.

‘Serious and organised investment fraud—colloquially known as ‘boiler-room’ fraud due to the high pressure sales tactics used—are usually initiated by cold calling potential victims. Serious and organised investment fraudsters target Australian investors with promises of high investment returns, backing up their claims with fraudulent websites to which the criminals can direct unsuspecting investors.

‘This type of fraud involves the illegal and often aggressive selling of worthless or overpriced shares. It is generally highly organised, spans multiple jurisdictions and uses sophisticated technology. This type of fraud also involves non-compliance with share-listing requirements, making fraudulent statements to shareholders and using false identities.

‘Typically based offshore, these investment frauds use the internet to conduct their illegal operations. They are incredibly sophisticated and very difficult for even experienced investors to identify.

‘Organised criminal groups are attracted to the high levels of superannuation and retirement savings in Australia.’

Source: <https://www.crimecommission.gov.au/organised-crime/crime-types/frauds>

Victim's story:

Tom's offshore investment in futures delivers devastating returns

The Hong Kong company I was dealing with operated as a broker for gold and oil futures on the UK exchange. They had very sophisticated and believable trading systems in place under the banner of Top Accrual Trading Systems complete with a very professional website, www.topaccrual.com. I have had 18 years of experience trading shares on the Australian Stock Exchange and the scheme seemed very realistic.

They initially contacted me via phone and then sent through glossy brochures which were really quite professionally put together. The returns on offer were at least 8 per cent better than I could get anywhere else and offered a short term three month investment turnover. I was provided constant updates and could track progress which showed my original outlay of \$35 000 had early returns well in excess of the initial forecast. My portfolio had increased in value to \$42 000 in just two months.

Towards the end of the first term I was offered an early bird opportunity to increase my portfolio for a second release but I would need to find at least \$60 000. With all going well on the first investment it was a simple decision. I invested the \$60 000 subsequently and later added another \$35 000, a total of \$130 000 in three transactions.

The first repayment of the investment was due on 18 May but didn't eventuate. I was given a myriad of reasons and excuses why the money did not arrive, mainly due to banking errors and clerical errors. There were further offers and opportunities to rollover my investments but I just wanted to cash out and consider my options. I pressed them for a pay-out but that was met with stone cold silence. Finally, the website and my money disappeared.

I have heard many stories of scams but none like this one. I have had a number of successful investing experiences, which unfortunately did influence my thinking to a degree, although clearly I should have done more research into the scheme in the first place.

'Scams don't just target the gullible and inexperienced. People from all walks of life can fall victim if the timing is right and the story is convincing. If you get a call out of the blue, ask yourself who you are really dealing with. Do your homework and visit moneysmart.gov.au for reliable advice on investing.'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. If you receive a phone call out of the blue, always ask for the name of the person you are speaking to and who they represent.
2. If someone offers you an investment or other financial service, ask for their Australian Financial Services Licence number and check this with ASIC.
3. Check the list of known cold-calling entities on Moneysmart.gov.au but remember that just because something is not listed doesn't automatically mean it is OK.
4. Do not let anyone pressure you into making decisions about money or investments: always get independent financial advice.
5. Be wary of investments promising a high return with little or no risk.

SCAMwatch radar: Don't be fooled by a fake business franchise



In February 2014 the ACCC issued a SCAMwatch radar warning would-be investors to carefully examine all documentation before entering into a franchise or business opportunity.

Franchising scams are often slick and professional, with a sophisticated website, marketing material and buzz-words. Scammers may also promote franchises as a golden opportunity for investors to join a 'proven' business that requires minimum effort, experience or skill with instant rewards.

If you are interested in joining a franchise, make sure you know what you're getting into—some business investment scams are little more than a highly sophisticated pyramid scheme and hard to tell apart from genuine offers. If you sign up to a fake franchise, you will lose your money.

Read more at www.scamwatch.gov.au.

#3. Computer prediction software and sports investment schemes

Number of scam reports:

487

Per cent of total reported loss:

11%

Per cent of total scams reported:

<1%

Number of consumers reporting losses:

256

Total losses reported by consumers:

\$9 039 340

Scam conversion rate:

53%

Most affected age group:

25-64 y.o. 88%

Gender:

Female: 27%

Male: 73%

In 2014 the ACCC received significantly fewer reports but almost the same amount of money was reported lost. Losses were still just above \$9 million dollars whereas the number of reports fell from 1087 in 2013 to 487 in 2014. The percentage of those reporting losses increased with the conversion rate climbing by 15 per cent to 53 per cent in 2014.

Scams in this category come in a variety of different guises. All are based on claims that they have developed software capable of accurately predicting results of sporting events, usually horse races, and often claim to be able to forecast share market movements. Some will sell the actual software and guide on how to use it while others will ask you to invest money into a syndicate, betting or growth account. They all emphasise and promise high returns or profits and play down the risk.

Not uncommon are claims of being able to run a sports arbitrage system where the scammers claim they have several people searching the global betting world to place bets at fixed odds. They claim that by doing this they can find different odds for either side of a sporting contest allowing them to bet on both participants and guaranteeing a win.

People who have 'invested' in these schemes report:

- the software or system does not work
- low or no returns are received
- the company cannot be contacted or refuses to deal with problems or inquiries.

Any claims of accurately predicting movements should be treated with extreme caution.

Victim's story:

Adam's taken for a ride on a horse betting scam

Adam received a glossy brochure extolling the benefits of investing in the sporting industry. There were plenty of facts and figures showing high returns and pictures of attractive people enjoying the high life at glamorous sporting events. All he had to do was buy the software, outlay \$20 000 and follow the program.

'The initial managed horse lay trading account cost \$20 000 but only made about \$2000, well short of the promised returns. I rang the helpline and was then offered the opportunity to upgrade to a better program for another \$25 000. I argued that the first program hadn't made anywhere near the promised \$20 000, so why would I invest another \$25 000?

'She argued that with the new program I could be making up to \$5000 a month on it.

'I argued that I hadn't even made my money back and you want to upgrade me.

'After several days of badgering I submitted to the upgrade. In due course, my betting account with Betfair was drained on several occasions after I had to top it up for them to keep betting.'

After many more calls to the helpline, Sharon would no longer return Adams phone calls.

'Enter Johnny, who rang and said if I could invest more funds to bring it up to \$70 000, the company would invest \$30 000 to make it \$100 000 for the corporate package. I hesitated a bit but was persuaded to do it. I ended up investing the full \$100 000 to which I was then informed that I needed to add \$25 000 for the betting or investment fund to work.

'I argued that nothing was said about another fund.

'He said well you need to do it or you lose the \$100 000.'

Adam reluctantly sent the \$25 000. A week later he was informed that he needed to pay another \$10 000 as he hadn't fully paid for an earlier upgrade.

'Again I argued that the system didn't deliver what they said it would do. They simply said that if I didn't pay, the system wouldn't work properly. I paid it, only to be told that I need to pay a hefty fee to release my funds. I didn't pay and was told "bad luck you lose it all".'

'Australians love a bet and scammers are quick to capitalise on this. However there is no such thing as a sure fire winner. Ask yourself, if you had a fool-proof way to predict a winner, why would you sell the secret?'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Be wary of high pressure and slick sales techniques. Do not let anyone push you into making decisions about money or investments—always get independent financial advice.
2. If you receive a call from a salesperson trying to sell you a sports investment 'opportunity'—just hang up!
3. Don't be enticed by reports of past performance or graphs showing high returns. Scammers lie!
4. Remember: no-one can guarantee that you will make money by gambling.

#4. Inheritance scams

Number of scam reports:

4358

Per cent of total reported loss:

5%

Per cent of total scams reported:

5%

Number of consumers reporting losses:

89

Total losses reported by consumers:

\$3 888 275

Scam conversion rate:

2%

Most affected age group:

55 and over 44%

Gender:

Female: 52%

Male: 48%

Inheritance scams have a very low conversion rate but represent over \$3.8 million in losses. While many scams are moving into the digital space, the classic approach of sending a letter is still the preferred method of delivery with almost 55 per cent of reports indicating the scam starts with a letter out of the blue. An indication that this may change in coming years is the fact that while the majority of reports show a letter as the contact mode used by the scammer, the lower numbers of email based contacts yields higher losses. In the case of letters, losses in 2014 were reported at over \$900 000 while e-mail based inheritance scams netted over \$1.7 million.

In either case, the initial letter or email will claim to be from a lawyer, usually in Europe, who has a late client who happened to share the same surname as the recipient. The letter states the lawyer has searched the globe for someone to share the inheritance with because if he does not find a rightful heir, no matter how distant, the government will take the inheritance as local laws dictate. The lawyer can get the money now that he has found an heir but in order for the process to appear legal, a series of fees and taxes must first be paid by the heir. The very low conversion rate suggests that the vast majority of people who receive such an offer dismiss it instantly. Those who consider the offer seriously and part with their money on average lose over \$40 000 each. Under the guise of filing paperwork and submitting applications to claim the inheritance, the scammer will often obtain a wealth of information from the victim. These often include photocopies of passports, bank account details, tax file numbers and Medicare numbers which can then be used for ID theft.

Scam survivor's story:

Leo gives away his life savings trying to gain an inheritance

Leo received a letter one day which claimed to be from a lawyer in Portugal. The letter seemed professional because it had a fancy letterhead and used legal jargon to explain a very interesting proposal. The letter offered Leo a share in a large inheritance which was left to the closest legal heir of the lawyer's late client. This client apparently had no immediate family in Portugal and efforts to find someone in Europe were fruitless. The lawyer then devised a scheme in which he could claim that Leo is a distant relative and the legal heir to the fortune since he shared a unique surname with his late client. In this way Leo and the lawyer could split the inheritance between them. Leo knew his surname was somewhat rare and the letter seemed to come from Portugal as claimed since the envelope had a Portuguese stamp on it.

Hoping he had come across a once in a lifetime offer, Leo contacted the lawyer to find out more and was soon convinced the scheme could work. In order to get the ball rolling, Leo would need to pay a few fees and taxes to make the process appear legal. Leo paid these fees which seemed to come one after another but each time he was assured he was closer and closer to receiving his share of millions of Euros. Every time he paid one tax, the lawyer would discover that some bank policy or quirk of local laws required another fee to be paid. At each step of the way, the lawyer claimed he too was putting in his fair share to pay these taxes and had invested a lot of his own money into the scheme. By the time he had sent over \$30 000, it became clear the requests for money and the excuses for why the scheme had not worked out were not going to end. Leo lost all his savings trying to gain an inheritance which never existed.

'These scams can be quite elaborate to convince you that a fortune awaits. This includes sending you a large number of seemingly legitimate legal documents to sign, forms to fill out and fake declarations. Check with a real lawyer who will be able to quickly spot the fakes.'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. If you are unsure about the legitimacy of an offer discuss the matter with a lawyer in your own city or town—do not seek advice from anyone recommended by the people who have sent the letter/email.
2. NEVER give credit card, online account details, or copies of important personal documents to anyone you don't know or trust and never by email.
3. If you think you have provided your account details, passport, tax file number, licence, Medicare or other personal identification details to a scammer, contact your bank, financial institution, or other relevant agencies immediately.

#5. Computer hacking scams

Number of scam reports:
4443

Per cent of total reported loss:
3%

Per cent of total scams reported:
5%

Number of consumers reporting losses:
328

Total losses reported by consumers:
\$2 252 292

Scam conversion rate:
7 per cent

Most affected age group:
35 y.o. and over 78%

Gender:
Female: 59 %
Male: 41%

Hacking scams seek to exploit the vulnerability of computer systems to search for information and data that can help the scammer perpetuate some other fraud.

In previous years, this category included any intrusion into a computer system including the installation of malware or seeking permission to remotely gain access to computer systems. The new classification system now identifies 'Remote access' scams and 'Ransomware and malware' scams as separate categories. Even with these categories removed, losses arising from hacking scams almost doubled. Reported losses in 2014 amounted to \$2 252 292, up from \$1 130 947 in 2013.

With the convergence of technology, hacking scams can now target computers, mobile phones or tablets and potential victims may be approached via email, text or through social media. They often ask you to follow a link to a fake mirror site. If you login using your account details and password the hacker has access to your legitimate account and whatever information they find can be used to commit further fraud in your name.

Anatomy of a hacking scam

In 2014 the ACCC received a number of reports about a business email compromise scam which targets Australian businesses by hacking email addresses and imitating suppliers. The scam involves targeting a supplier or buyer and hacking into either or both of their computer systems to gain access to contacts and email addresses. They then work out the business relationship by looking over customer lists, bank details and previous invoices.

An email is sent from the supplier's email account to the buyer requesting a change to payment arrangements and asks for the invoice to be paid via wire transfer or to a new bank account the scammer has set up. The unsuspecting buyer updates the new payment arrangements thinking it is a legitimate request and then pays the scammer for the goods, leaving the supplier out of pocket.

Sometimes the scammer can hack enough information to identify a specific business relationship but cannot hack the supplier's email account. In such cases the scam can still work when the scammer creates a new email address which mimics the supplier's address and uses their logos and message format.

The victim company often does not detect the scam until they are alerted by complaints from the supplier that payments are overdue.

The Canadian Better Business Bureau and the United States Internet Crime Complaints Centre issued warnings about this scam operating in the northern hemisphere and, like other scams, it migrated south. In the latter half of 2014 Australian businesses started reporting this scam with one reported loss of over \$100 000. While the number of reports for these scams is low, reported losses are generally significant with many affected businesses losing in excess of \$10 000.

Victim Story:

John updated supplier details and ended up costing his company thousands

John worked as an accounts manager for a local manufacturing business. Late on a Friday afternoon, he received an email which appeared to be from Mr Liu from Zhang-Fei Industries, a ball bearings supplier in Asia. Mr Liu's email explained that due to a change in their internal finance system, he needed to update the banking details. John took the email at face value and changed the banking information in his company's database. A few days later, John made a scheduled transaction to Zhang-Fei Industries for \$17 000.

Two weeks later the ball bearings from Zheng Fei industries had not arrived so John telephoned Mr Liu. Mr Liu said he hadn't received payment for the last order and had consequently cancelled shipment. John told Mr Liu that he had processed the payment personally to make sure it was paid according to the new arrangements. After some investigation it became clear that Mr Liu had not sent any request to update his company's banking details and John had fallen victim to a scam.

In the weeks to come, with the initial loss of \$17 000, the delay in supply flowing from missed orders and broken contractual obligations, John's company estimated their loss to be over \$30 000.

“Effective management systems and safeguards to prevent access to your computer should be an integral part of any business, large or small. Often very simple common sense procedures like double checking accounts over a given threshold amount could save thousands of dollars.”

ACCC Deputy Chair Dr Michael Schaper

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Make yours a 'fraud-free' business—effective management procedures can go a long way towards preventing scams. Have a clearly defined process for verifying and paying accounts and invoices.
2. Consider a multi-person approval process for transactions over a certain dollar threshold.
3. Double check email addresses—scammers can create a new account which is very close to the real one; if you look closely you can usually spot the fake.
4. If you think a request is suspicious, especially any request to change bank account details, telephone the business to seek verification of the email's authenticity and cross check with internal records you already have on file.
5. Check your IT systems for viruses or malware—always keep your computer security up-to-date with anti-virus and anti-spyware software and a good firewall.

#6. Nigerian scams

Number of scam reports:

1053

Per cent of total reported loss:

3%

Per cent of total scams reported:

1%

Number of consumers reporting losses:

86

Total losses reported by consumers:

\$2 193 094

Scam conversion rate:

8%

Most affected age group:

Over 25 y.o. 92%

Gender:

Female: 51%

Male: 49%

In 2014 this perennial scam continued to attract victims who parted with just over \$2 million. Its relatively low conversion rate suggests most of us are aware of these approaches that promise millions but never deliver.

Despite their name, 'Nigerian scams' can come from anywhere in the world. Originally coming from Nigeria, the scams are also referred to as '419' scams, taken from the section of the Nigerian Criminal Code outlawing the practice.

They are a form of upfront fee scam in which the scammer claims a wealth of money is trapped in a bank due to a local conflict or left behind by a corrupt politician from a former despotic regime. Often the story will reference real world events. The scammer claims they are desperately looking for someone to provide bank account details so they can offload the money to a safe country and, as a reward, they will share the wealth when it is safe.

However, like any upfront fee scam, the scammer soon asks for money to be paid before the transfer can be processed. These usually come in the form of requests to pay fake taxes and fees to meet 'international banking regulations' or 'anti-terrorism and money laundering laws'. By the end of such a scam, a host of characters have been introduced ranging from lawyers to banking officials to high ranking members of the United Nations, all of whom require payment before the funds can be released.

Typical Nigerian scam approach

Dear friend.

Greetings to you and your family, I am the manager of bill and exchange in THE BANK, I have a business of 5.5 million United State dollars to be transfer to your account for investment in your country, if you are ready to assist me get back to me, I will give you full details on how the fund will be transfer to you.

Be rest assured that everything will be handled confidentially because, this is a great opportunity we cannot afford to miss, as it will make our family profit a lot.

It has been seven years ago and most of the politicians are no longer in power again and they don't use our bank to transfer funds overseas anymore since their tenure had expired.

The \$5.5 million United State dollars has been lying in the bank as unclaimed fund and I will soon retire from the bank immediately the fund is transfer into your account over there.

Immediately the fund has been successfully transfer into your account I will come to your country for the sharing of the fund, the fund will be shared 50 per cent for me and 40 per cent for you, and the other 10 per cent for the orphanages home and poor with less-privilege people.

Please note that if you must get in touch with me then you must reply me back through my private box (ramar.XXXX1@laposte.net) and please if you are not interested do not waste your time to reply kindly delete my message from your box ok.

Waiting to hear from you soon.

Yours faithfully,

Mrs.Rama XXXX

'If you receive an approach like this, delete it or throw it in the bin.'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Remember there are no get-rich-quick schemes: the only people who make money are the scammers.
2. Do not open suspicious or unsolicited emails; delete them.
3. NEVER reply to a spam email (even to unsubscribe).
4. Money laundering is a criminal offence: do not agree to transfer money for someone else.

#7. Fake trader websites

Number of scam reports:
2093

Per cent of total reported loss:
3%

Per cent of total scams reported:
2%

Number of consumers reporting losses:
1369

Total losses reported by consumers:
\$2 134 163

Scam conversion rate:
65%

Most affected age group:
25-44 y.o. 53%

Gender:
Female: 56%
Male: 44%

In 2014 scammers continued to target Australians buying and selling in the online retail market. Online shopping on fake trader websites represented only 2 per cent of all scam contacts yet just over \$2 million dollars was reported lost.

Because of changes to scam classifications in 2014 there is no comparable data for previous years. Previously this type of scam was included in a broader online shopping category that included classified ad scams and online auction sites. This category now only focusses on those sites that are deliberately set up to impersonate an existing site or operate for a short period of time for the express purpose of accepting online payments for goods or services with no intention to supply.

Scammers can easily produce convincing looking websites that are clearly successful in tricking people into handing over their money. The conversion rate of 65 per cent means well over half of the people who reported losing money to a fake website were convinced they were dealing with a legitimate trader.

Some scams actually cold call their victims and direct them to the website or lure people in with attractive offers in an email that links directly to the fake site.

It is one thing to set-up a fake website, but far more difficult to establish a creditable payment facility. If a website asks for payment by wire transfer, cheque or money order, steer clear.

Scammers know to target popular consumer goods where there is high demand, low supply levels or high prices.

Common products that scammers use when 'buying' or 'selling' online include holidays, hotel accommodation, electronic items such as smart phones, tablet devices and laptops or high end photographic equipment.

For online shoppers, tell-tale signs of a scam is a sought-after item at a price that seems too good to be true and being asked to pay by something other than a credit card, e.g. via Western Union or Moneygram.

SCAMwatch report: Fiona's better judgment

Fiona had been searching online for photo developing equipment and supplies which had become increasingly difficult to source at a reasonable price since the shift to digital photography.

A message on her Facebook page showed that a friend had 'liked' a website that offered what she was looking for.

'I followed the link which took me to a well-constructed site complete with catalogue and price list. The prices were very competitive but the company was based in China. I hadn't bought from overseas companies before but was re-assured when I saw delivery to Australia was relatively cheap and the overall savings on buying the same thing locally still meant I would save 25 per cent.'

On ordering the products Fiona was asked to use Western Union or Money Gram to pay for the items. When she enquired about PayPal or payment by credit card they made up a story about an audit that was taking place. They told Fiona she would have to wait a month unless she used a wire transfer service like Western Union, Moneygram or a service she hadn't heard of called UKash.

Fiona was suspicious so before sending any money she sent an email asking more about the audit situation and delivery arrangements. No response was received. Fiona then contacted her friend who had liked the website only to be told they knew nothing about the website and had never used it.

Fiona logged on to SCAMwatch and quickly discovered the website had all the signs of being a scam. Following advice she read on SCAMwatch, Fiona conducted a quick Google search of the website's URL. This quickly revealed others had been caught out.

Fiona reported the details to SCAMwatch and said: 'I am reporting this because the web page and catalogue were presented very professionally and someone may lose substantial money.'

'Fiona's report and those of all the people that report to SCAMwatch helps to keep the site relevant and up to date on the latest scams targeting Australians.'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Don't trust the legitimacy of an ad just because it has the name of a company you know and trust—scammers often use these to lure you in but then direct you to their fake website.
2. Do not open suspicious or unsolicited emails (spam): delete them.
3. Do not click on any links in a spam email, or open any files attached to them. Independently source the details of the website and type in the URL address yourself.
4. Where possible, avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer or international funds transfer. It is rare to recover money sent this way.
5. Do an internet search using the exact wording in the ad—many well-known scams can be found this way.

SCAMwatch radar: Don't let scammers kick goals in the lead up to the 2014 FIFA World Cup



In March 2014 SCAMwatch and FIFA warned soccer fans seeking to buy tickets to the 2014 FIFA World Cup in Brazil to beware of websites selling fake tickets.

Those wishing to purchase tickets were advised that official and guaranteed tickets could only be bought via www.FIFA.com—no other websites or parties were authorised to sell tickets.

Past international events saw similar scams where websites appeared to be legitimate and professional. Fans were warned that scammers might even set up websites that use the official '2014 FIFA World Cup Brazil' logo and trademarks (or their look-alikes) to lure them in to thinking the site is official and that it's an authorised seller.

Read more at www.scamwatch.gov.au.

#8. Classified scams

Number of scam reports:

3218

Per cent of total reported loss:

2%

Per cent of total scams reported:

4%

Number of consumers reporting losses:

782

Total losses reported by consumers:

\$1 950 366

Scam conversion rate:

24%

Most affected age group:

25-54 y.o. 67%

Gender:

Female: 47%

Male: 53%

Classified ad scams typically involve a scammer posting a fake ad on a legitimate classifieds website for well priced goods such as cars, boats, caravans and pedigree pets. If a recipient shows interest in an item, the scammer will claim that the products will be delivered following receipt of payment. If the recipient pays, they will lose their money, not receive the products nor be able to contact the seller.

The scam works both ways. A scammer could express interest in an item you have advertised and ask you to send them the goods. They have been known to pay for items by using fake cheques, stolen credit cards or even forged copies of Paypal receipts.

In 2014 Australians lost nearly \$2 million dollars to scams like this.

Classified sites are different to many other online auction and shopping sites and are designed to offer a simple service that puts legitimate buyers and sellers together. They generally don't have payment options or escrow services. If you can't inspect the goods or receive the cash-in-hand then classified advertising is probably not the right service for you.

Victim's story:

Alex avoids being taken for a ride by a scammer

Alex, who lives in Melbourne, advertised his car for sale on a popular online classifieds site for \$5000. The following day he received an email from Brian who said he was interested in buying the car. In fact, Brian was happy with the going price as the car was exactly what he was after.

Alex was ecstatic as he had only just advertised the car, and thought it would take a lot longer to find a buyer. He asked Brian when he would like to come inspect the car and take it for a test drive. To his surprise, Brian replied that he was not able to inspect the car as he was currently working as an engineer offshore from New Zealand. However, Brian was still keen to go ahead with the purchase as it was exactly what he was after, and he would arrange for the car to be shipped to him.

Brian asked for Alex's PayPal account details so that he could transfer the money. Brian also informed Alex that the shipping company he wanted to use to ship the car from Melbourne to New Zealand would only accept payment from the seller. Therefore, Brian would transfer \$6000 to Alex via PayPal—\$5000 for the car and \$1000 to cover shipping costs—and Alex would then need to send \$1000 to the shipping company via wire transfer.

Alex provided Brian with his PayPal account details, and Brian provided him with the details of where to transfer the money for the shipping costs.

The following day Alex received an email from what appeared to be PayPal saying that \$6000 had been transferred into his account. The email had all the logos and branding associated with PayPal. Alex was just about to begin transferring \$1000 to the shipping company when he was struck with the thought, 'Why would someone buy a car without inspecting it first?' He then checked his PayPal account and found that no money had actually been transferred into it. He also noticed that the email from PayPal had not come from the usual PayPal email address. He then called the shipping company and was told that the number had been disconnected.

Alex realised that he had almost fallen victim to a scam. He called PayPal and provided details of what had happened.

'If you are looking to sell something online, never accept money that is more than what you agreed upon for the item's price—it's a tell-tale sign that the 'buyer' is in fact a scammer.'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Be cautious—if the advertised price of a good, service or rental property looks too good to be true, it probably is.
2. Don't trust the legitimacy of an ad just because it appears in a reputable newspaper or classifieds website—scammers post fake ads in these too.
3. If you are buying, only ever pay when you have received the goods.
4. If you are selling online, be very wary of any buyer who only wants to pay by cheque, money order or money transfer—wait until the money is actually credited to your account by the bank before sending the goods.

#9. Unexpected prize and lottery scams

Number of scam reports:
3315

Per cent of total reported loss:
2%

Per cent of total scams reported:
4%

Number of consumers reporting losses:
271

Total losses reported by consumers:
\$1 890 265

Scam conversion rate:
8.2%

Most affected age group:
45 y.o. and over—53%

Gender:
Female: 55%
Male: 45%

In 2014, unexpected prize and lottery scams continued to score wins against Australians. The ACCC received 3315 reports for this scam type with reported losses of \$1 890 265.

The conversion rate for this type of scam has increased from 6 per cent in 2013 to 8 per cent in 2014. While a low conversion rate suggests most people do not believe they can win millions in a lottery without first buying a ticket, a more targeted approach by scammers through the use of social media may explain the increase this year. Reports to the ACCC indicate unexpected prize scams delivered through Facebook have won scammers almost \$400 000 or just over 20 per cent of the losses in this category.

Victims described receiving messages which appear to be from friends telling them that they too have won money and it has worked out for them. With this personal assurance from a trusted source that the lottery is real, victims part with their money hoping they too can share in the winnings. From this point, the scam follows the predictable pattern of requesting upfront payments before the prize money can be released. The targeted use of social media in this way is a good example of how scammers adapt age old scams to emerging communication platforms.

Another scam in this category reported in 2014 involves an offer of vouchers in exchange for answering a survey. Typically the vouchers purported to be redeemable at major brand outlets such as Bunnings, Woolworths, Coles, IGA and JB Hi-Fi and offered between \$150 to \$1000 worth of credit to spend in store. Before the voucher can be received, a survey must first be completed. However, the voucher is either fake or it simply never arrives, and the surveys are not affiliated in any way with the actual businesses.

Some victims lost money to this scam when they provided their mobile phone numbers and were subsequently signed up to a premium messaging service which they often did not realise until receiving their phone bill. A far greater number of reports indicate no monetary loss but were concerned about the loss of personal information. Much like marketing companies, scammers are using these surveys to obtain personal details which in turn are used for future scam attempts. Many of the reports received by the ACCC indicated that, following participation in a survey, victims found themselves inundated with a range of scam emails.

Scammers in 2014 proved their ingenuity and ability to change with the times by continuing the shift of scams from telephone calls and letters to the online space. Scammers adopt the same marketing techniques legitimate businesses use to reach out to consumers through online promotions and social media campaigns. Consumers need to be ever more vigilant with their personal data and be sure of whom they are dealing with before parting with it.

Victim's story:

Davin

Davin received a private message on Facebook from the 'Facebook Freedom Lottery' claiming he and 20 other winners could claim various amounts up to \$150 000. At first he didn't believe it. Businesses don't give money away out of the blue and to win in a lottery you need to buy a ticket. However, moments later his cousin who he hadn't spoken to in some time sent him a Facebook message about the winnings. Davin's cousin claimed that he had also won and noticed Davin's name on the list of winners. He claimed he had already received his winnings after going through a relatively easy process.

Trusting his cousin, Davin began the process for accepting the prize money which required him to first pay a small upfront fee of \$250. Once this was paid, he was to receive the money into his nominated bank account for which he provided details. The next day he was informed that since the prize money was sitting in a bank in the USA, he would have to pay an 'international transfer fee' which could not be subtracted from the winnings for some complex legal reason. Davin reasoned that since his cousin had managed to receive the money, then he must have gone through the same process and so he would also pay this additional fee.

Over the next two weeks, Davin paid five more fees, each time believing it would be the last. Eventually, in desperation, he spoke to his cousin and asked how many fees he paid before he received his winnings. Davin's cousin had no idea what Davin was talking about and told him that he had only just regained control of his Facebook account after it had been hacked.

It then became clear to Davin that he had been scammed. There never was any prize money and the Facebook message was part of the scam. By this time, Davin had already sent \$1500 and handed over a wealth of personal information to scammers.

'Don't let scammers win the ultimate lottery by gaining your personal details and money—if something seems too good to be true, it probably is.'

ACCC Deputy Chair Delia Rickard

* All names have been changed and aspects are drawn from real examples for illustrative purposes.

PROTECT YOURSELF TIPS

1. Remember: you cannot win a lottery or competition unless you entered it.
2. Ask yourself who you're really dealing with—scammers pose as legitimate organisations to make them appear to be the real deal.
3. Before providing any personal details in a survey, check first that an offer of vouchers in return for your information is legitimate by contacting the business directly.

SCAMwatch radar: Automated scam calls claiming to be from Qantas with bogus holiday win



In August 2013 the ACCC issued a SCAMwatch alert warning people about automated calls from scammers posing as Qantas staff claiming that they've won a credit towards their next holiday.

The message said that because the person has recently booked a flight with Qantas, they have won a 'travel prize' or 'credit points'—typically \$999—towards their next holiday.

In order to redeem the credit, the person is directed to press '1'. At this point, the person is put directly through to a scammer, who will then state that in order to be eligible for the prize they will first have to answer a few questions. The scammer may ask whether the person is aged over 30, whether they have a valid credit card, and finally ask for their credit card details so that the prize can be processed.

Once credit card details are provided, money is taken from the account.

Read more at www.scamwatch.gov.au.

#10. Overpayment Scams

Number of scam reports:
1293

Per cent of total reported loss:
2%

Per cent of total scams reported:
1%

Number of consumers reporting losses:
188

Total losses reported by consumers:
\$1 521 374

Scam conversion rate:
15%

Most affected age group:
25–34 y.o. 29%

Gender:
Female: 49%
Male: 51%

Overpayment scams target small businesses and individuals, anyone that has something to sell. In 2014, two thirds of the losses reported were from small businesses and accounted for just over \$1.5 million. Scammers generally targeted businesses selling stock and equipment.

Most commonly the small business receives an email from the scammer requesting to purchase goods but sometimes also services. The scammer provides the business with several credit card numbers to pay for the goods but also asks that extra money be deducted from their credit card and to transfer this money via money transfer to cover the fees of an agent or extra shipping costs. Eventually the business is advised by their bank that the credit cards were stolen. If goods are sent then the business loses not only the amount of any money sent but also the loss of stock.

PROTECT YOURSELF TIPS

1. Make yours a 'fraud-free' business—effective management procedures can go a long way towards preventing scams. Have a clearly defined process for verifying and paying accounts and invoices.
2. Make sure that cheques or credit card transactions have been cleared by your bank before transferring or wiring any refunds or overpayments back to the sender.
3. If you think a request is suspicious, independently check business details and do a search online to check for similar scams.

5. Research

Research plays an important role in dealing with scams activity, helping to form a better understanding of how scams operate, the scale of activity, their impact on victims and emerging trends.

Scams-related research is critical in informing the ACCC and other law enforcement agencies' strategies to tackle scams activity so that these efforts are as effective as possible in addressing the conduct.

This chapter outlines some key recent and upcoming research undertaken around scams.

5.1 Australian Institute of Criminology research

The Australian Institute of Criminology (AIC) released two scam related pieces of research in 2014. The first looks at victims of fraud while the other examined identity crime

Challenges of responding to online fraud victimisation in Australia⁴

The study found that 'while victims of online fraud experience levels of harm similar to other victims of crime, they are often not seen as being legitimate victims. For most online fraud victims, this stems from the unique characteristics of the crime perpetrated against them that makes conventional criminal justice responses difficult or impossible.'

While the need to provide support services for victims of online fraud is clear, the very few dedicated services that are available show that further attention to the problem is needed. ... Further research into specifics around the needs of online fraud victims is currently being undertaken by the authors to address the issues identified in this paper and further to inform the evidence base on this important topic.'

Identity crime and misuse in Australia: Results of the 2013 online survey⁵

In May 2013 the AIC was commissioned by the Attorney-General's Department to undertake a national survey. The report, released in 2014, confirmed prior research that found identity crime affects a relatively high proportion of Australians who report substantial financial and other impacts. Identity crime and misuse of personal information affect all sectors in Australia and cost individuals, business and government many millions of dollars annually.

5.2 Attorney-General's Department: Identity security

On 21 October 2014, the Minister for Justice, the Hon Michael Keenan MP, released the first report from the National Identity Crime and Misuse Measurement Framework project. The report⁶ 'brings together available data from over 50 different Commonwealth, state and territory agencies, as well as the private sector, to make a series of key findings on the nature and extent of identity crime in Australia.'

The report noted that 'identity crime is one of the most prevalent criminal activities in Australia, affecting hundreds of thousands of Australians every year. Criminals can generate significant profits by stealing personal identity information, then manufacturing or selling fraudulent identity credentials to defraud businesses, individuals and financial institutions. Criminals also use these illicit identities to access government benefits and services to which they are not entitled.'

The economic impact of identity crime in Australia is estimated by the report to exceed \$1.6 billion dollars annually.

4 *Challenges of responding to online fraud victimisation in Australia*, Cassandra Cross, Russell G Smith & Kelly Richards, Australian Institute of Criminology, May 2014.

5 *Identity crime and misuse in Australia: Results of the 2013 online survey*, Russell G Smith, Alice Hutchings, Australian Institute of Criminology, May 2014.

6 *Identity crime and misuse in Australia: Key findings from the National Identity Crime and Misuse Measurement Framework Pilot*, Attorney General's Department, October 2014.

5.3 Upcoming Australian Bureau of Statistics' personal fraud survey

In 2013 the Australian Bureau of Statistics (ABS) commenced work on the 2014–15 personal fraud survey.

This national survey is a key piece of work in helping to understand the scale of scams activity across the country, with comprehensive data from the populace providing a detailed overview of the number of people in Australia affected by scams, the nature of scams and their impact.

The most recent report, *Personal fraud survey 2010–11*, found that Australians lost \$1.4 billion due to personal fraud (which includes credit card fraud, identity theft and scams).

The results of the 2014–15 survey will be released in 2016.

6. Education and awareness raising initiatives

The ACCC uses a range of tools to protect consumers from scams, with education and awareness raising a key pillar in its efforts to minimise the impact of scams on society.

Scams present a considerable challenge for law enforcement agencies, with the perpetrators often frustrating traditional regulatory approaches by setting up schemes that are difficult to trace, based overseas and cross multiple jurisdictions. Scammers take advantage of instant and anonymous communication channels to connect with targets, and are quick to morph and phoenix operations into a new scam when authorities close in.

Education and awareness raising therefore plays a key role in preventing harm arising from scams activity, by empowering individuals with the knowledge and skills to identify and avoid victimisation in the first instance.

This chapter outlines ACCC initiatives to help the Australian community protect themselves from scams.

6.1 SCAMwatch

The ACCC runs the Australian Government's SCAMwatch website (www.scamwatch.gov.au), which provides the public with information and advice on how to recognise, avoid and report scams, as well as what to do if one thinks that they have been scammed. Consumers and small businesses can also receive information over the phone through the SCAMwatch hotline.

SCAMwatch has significant brand awareness amongst the community with the Australian Government, state and territory government departments, media, consumer groups and private companies directing people to the website for information on scams. SCAMwatch is also considered a valuable resource internationally, with a number of regulators in overseas jurisdictions including Canada, New Zealand, and the United Kingdom referring consumers to the site.

SCAMwatch also operates as the web portal for the Australasian Consumer Fraud Taskforce, promoting Taskforce initiatives such as its annual National Consumer Fraud Week campaign. More information about the Taskforce is provided at section 7.1.

In 2014 the SCAMwatch website received 1 336 869 unique visitors, an increase of 108 270 or 9 per cent from 2013. Figure 7 shows that SCAMwatch visits have consistently trended upwards since the ACCC assumed responsibility for the site in 2006, with an increase in visits of over 70 per cent since 2011.

Although the majority of visitors were located in Australia, SCAMwatch was also visited by people located around the world. Significant numbers of visitors came from the United States, United Kingdom and Canada which collectively accounted for approximately a third of all visitors.

Figure 7: Unique visitors to the SCAMwatch website from 2006 to 2014

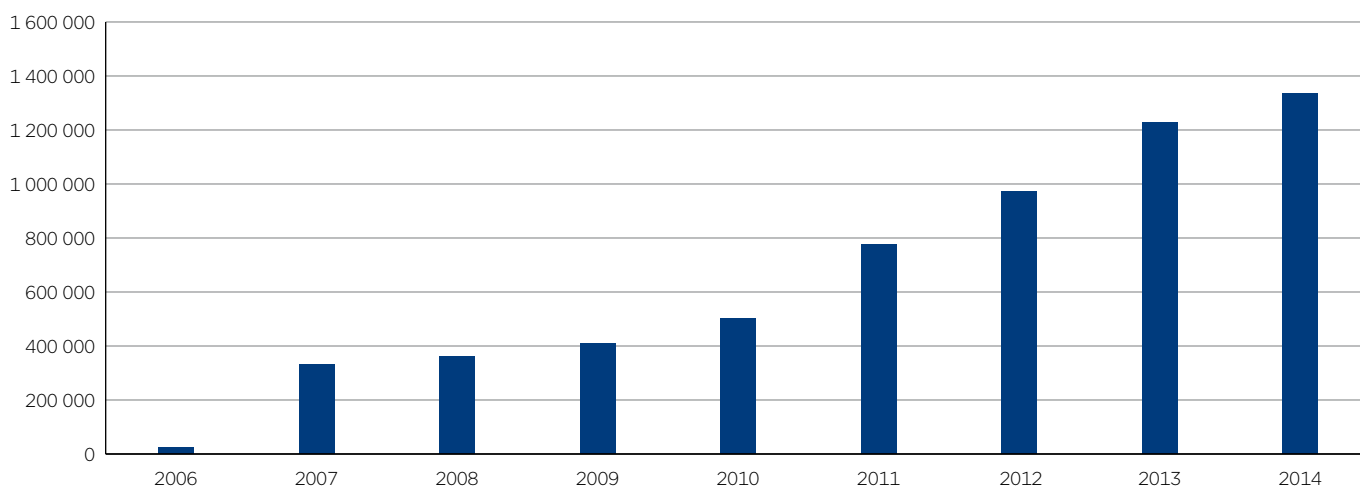
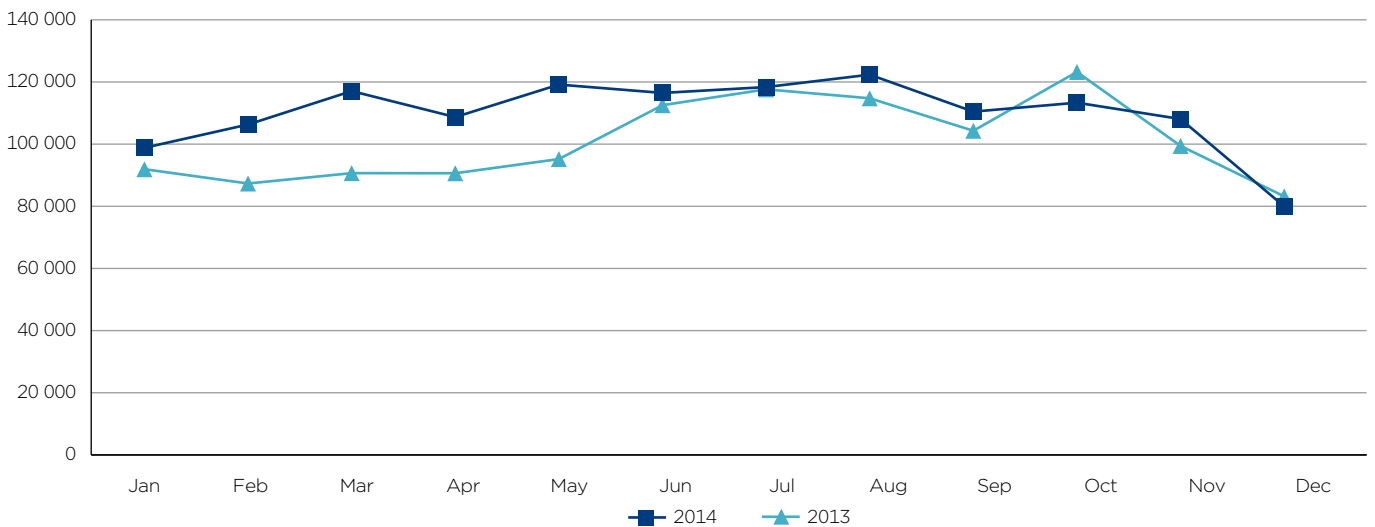


Figure 8 shows that in 2014 SCAMwatch attracted on average more unique visits per month compared to 2013, with the exception of a slight decline in October. Typically, unique visits to the SCAMwatch site decline over the Christmas period and this has been a consistent trend over a number of years.

Figure 8: Comparison of monthly visits to the SCAMwatch website in 2013 and 2014



SCAMwatch radar alert service

The ACCC also runs a free SCAMwatch subscription service whereby subscribers receive email alerts, known as ‘SCAMwatch radars’, on emerging scams.

In 2014 the subscriber network reached 36 165 subscribers, an increase of 24 per cent from 2013.

The ACCC issued 17 SCAMwatch radars in 2014 to warn Australians about the imminent risk of scams, including those relating to current events such as Valentine’s Day, tax time, ticket sales for the 2014 FIFA football world cup in Brazil, and the Malaysian Airlines MH370 and MH17 tragedies.

SCAMwatch radar alerts are also an effective mechanism for a collaborative approach between government and industry to alert the public to scams targeting customers or particular community groups. For example, in July 2014 the ACCC and the Australian Taxation Office issued a joint alert to warn Australians about tax refund scams. In September 2014, indigenous consumers were warned about an advance fee fraud targeting remote and rural communities in northern Queensland.

A full list of SCAMwatch radar alerts issued in 2014 is provided at appendix 3.

Don’t let scams slip under your radar! Sign up to the SCAMwatch alert service

The ACCC has a free SCAMwatch subscription service where you can sign up to receive email alerts on new scams doing the rounds.

Sign up to receive SCAMwatch radar alerts at www.scamwatch.gov.au.

SCAMwatch Twitter—@SCAMwatch_gov

The ACCC also communicates with the public via its SCAMwatch Twitter profile—@SCAMwatch_gov. This social media platform allows SCAMwatch to reach consumers, small businesses and the media in real time as scams emerge.

In 2014 SCAMwatch Twitter posted 539 tweets to its 7721 followers on the following topics:

- alerts on emerging and current scams
- information exposing scammers’ tactics
- tips to outsmart scammers and protect oneself
- how to report a scam
- what to do after being scammed.

Join the SCAMwatch Twitter community

Follow SCAMwatch on Twitter to receive timely alerts on scams targeting Australians

Visit https://twitter.com/SCAMwatch_gov or @SCAMwatch_gov.

6.2 Other scams educational resources

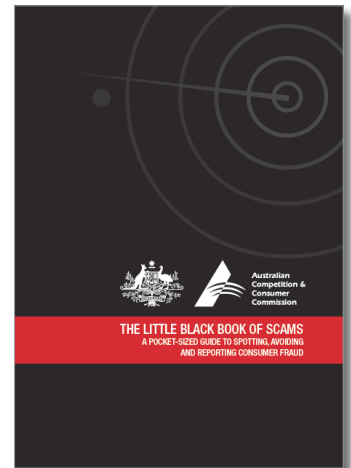
The ACCC has also produced a range of educational resources to educate consumers and small businesses about how to identify a scam and avoid being duped. Additional scam related resources for consumers and businesses are also noted in Appendix 4.

The Little Black Book of Scams

The ACCC's *Little Black Book of Scams* is its primary educational resource, and the ACCC's most popular publication. In 2014 over 108 000 copies of the book were distributed throughout the community. The electronic publication was also downloaded 4041 times.

This publication highlights the most common scams that target Australians such as advance fee fraud, fake lotteries and sweepstakes, dating and romance scams, computer hacking and online shopping scams. It also explains scam delivery methods, tools used by scammers to trick people, personalised scam approaches, and golden rules on how to protect oneself.

The *Little Black Book of Scams* is considered a best practice educational resource internationally, with several overseas regulators producing their own localised versions.



Small business scams factsheet launched

In April 2013 the ACCC released *What you need to know about: small business scams*, a factsheet for small businesses on common business scams and how to avoid them.

The factsheet explains overpayments scams, directory entry or unauthorised advertising scams, investment scams, office supply scams, domain name scams, and email intercept and ransomware scams. It also provides a list of steps that businesses can take to help prevent being scammed.

The factsheet was downloaded over 500 times in 2014.



6.3 Media and communications activity

The ACCC recognises the important role of the media in helping to raise community awareness about scams activity. In 2014 the ACCC continued to proactively generate media interest in scams targeting Australians.

The Australasian Consumer Fraud Taskforce's National Consumer Fraud Week campaign is the key annual public awareness raising initiative for the ACCC. As with previous years, the release of the *Targeting scams* report during Fraud Week received significant media coverage in 2014.

Throughout the year, ACCC spokespeople engaged in over 200 scam-related interviews for print, radio and TV reaching a wide audience across the capital cities, remote Indigenous communities, and rural and regional Australia. This activity was supported at the local level by the inclusion of scams information in a number of business presentations.

The ACCC also continued to raise community awareness of scams activity through the 'Scam of the month' initiative (see highlight box).

ACCC 'Scam of the month' initiative continues to raise awareness about scams

In 2014 the ACCC continued its 'Scam of the month' initiative as a key part of its strategy to raise the profile of scams amongst the Australian community by way of media activity.

Each month, the ACCC selected a scam of particular concern to warn the public about and developed newsworthy and timely content to maximise media coverage. For example, Valentine's Day saw a warning to those looking for love online to watch out for dating and romance scams. In March the ACCC warned football fans to beware of fake websites selling FIFA World Cup tickets. July provided a caution about tax scams for people preparing their tax returns. In October, the public was warned about travel scams as they made preparations for their Christmas and summer holidays.

The ACCC worked closely with news outlets to generate media coverage of this initiative. This media engagement helped the ACCC to reach a broad cross-section of the community with scam warnings.

7. Domestic and international collaboration

The ACCC recognises that combatting scams is a shared responsibility between government, industry and individuals. At the government level a coordinated response is required, with collaboration between local and overseas entities essential to effectively deal with the global reach of scams.

Law enforcement agencies in both Australia and overseas face the same challenges that arise from scam operations having the capacity to reach consumers across jurisdictions with just the click of a button. Scammers often rely on legitimate platforms or communications channels to achieve a global reach, taking advantage of popular and trusted mediums to deliver the scam. As noted in the previous chapter, collaboration with business enablers to disrupt or disable scams activity is a critical component of disruption activity, in addition to working with overseas law enforcement agencies.

This chapter outlines ACCC efforts to collaborate with domestic and international agencies, and industry stakeholders, to prevent or minimise scams.

7.1 The Australasian Consumer Fraud Taskforce

The Australasian Consumer Fraud Taskforce was established in 2005 and comprises of 23 government member agencies across Australia and New Zealand that share a responsibility for consumer protection in relation to fraud and scams activity.

The Taskforce's main functions are to:

- enhance the Australian and New Zealand governments' enforcement activity against fraud and scams
- share information and research on consumer fraud and scams
- develop coordinated consumer education initiatives to raise community awareness about scams.

The ACCC's Deputy Chair, Delia Rickard, is the Chair of the Taskforce. The ACCC also provides secretariat services to the Taskforce.

The Taskforce's work is assisted by a number of government, business and community group partners. Partners recognise the seriousness of consumer fraud in Australasia, and play an important role in disrupting scams activity and raising community awareness.

National Consumer Fraud Week

A key initiative of the Taskforce is the annual National Consumer Fraud Week campaign, a coordinated effort by the Taskforce and its partners to raise community awareness about scams. Fraud Week supports the International Consumer Protection Enforcement Network's Global Fraud Prevention initiative.

2014 campaign—'Know who you're dealing with'

The 2014 Fraud Week campaign, 'Know who you're dealing with', ran from Monday 16 June to Sunday 22 June and focused on relationship scams. The campaign asked Australians to take a step back and think about whether someone they met online is the real deal, particularly if they ask for money.

Scammers are highly skilled at developing a relationship with people, using all sorts of tricks to connect with them and convince them to part with their personal details or money. The key message of the campaign was: 'think twice before transferring money—if someone asks for money, but you've never met them in person, they're more than likely trying to scam you'.

Campaign highlights included:

- the release of the ACCC's 2013 *Targeting scams* annual report
- the production and distribution of postcard tips on how to identify, avoid and disengage from scammers and
- the production of a 'Scam of the month, video about relationship scams and how to identify a scammer (see: <http://www.scamwatch.gov.au/content/index.phtml/itemId/1147995>).


The launch of the ACCC's fifth *Targeting scams* report generated significant media interest, which was used to promote Fraud Week. In the first two days of the campaign, Fraud Week was covered by nearly every major newspaper and radio station, focusing on the financial losses arising out of relationship scams reported to the ACCC. Further media focusing on small business scams also received coverage.

The fraud week campaign was supported by partners from a diverse range of backgrounds including government, business, community groups and industry bodies. Key areas relating to the theme were targeted including online shopping service providers, online and computer bodies, and the financial industry.

Figure 9 provides an outline of the 'Know who you're dealing with' campaign messaging.

Figure 9: 2014 National Consumer Fraud Week campaign messaging

KNOW WHO YOU'RE DEALING WITH



Friend or foe? **Think twice before transferring money.**

National Consumer Fraud Week 16–22 June 2014
An Australasian Consumer Fraud Taskforce initiative

Have you ever wondered if someone is the real deal? National Consumer Fraud Week 2014 is all about learning how to identify, avoid and disengage from scammers.

Know who you're dealing with—follow the 'Top 5 Scam Identifier' list:

1. You've never met or seen them: scammers will say anything to avoid a 'face-to-face' meeting, whether it be in person or over the internet via a video chat—don't excuse it away.
2. They're not who they appear to be: scammers steal photos and profiles from real people to create an appealing facade. Run a Google Image search on photos and search words in their description to check if they're the real deal.
3. They ask to chat with you privately: scammers will try and move the conversation away from the scrutiny of community platforms to a one-on-one interaction such as email or phone—'walk away' if this happens to you.
4. You don't know a lot about them: scammers are keen to get to know you as much as possible, but are less forthcoming about themselves. Ask yourself, 'how well do I really know this person?'
5. They ask you for money: once the connection's been made—be it as a friend, admirer, or business partner—scammers will ask you to transfer money. Don't fall for a tall tale, no matter how plausible it sounds.

Think twice before transferring money

If you meet someone online and they ask for any money, big or small, you are dealing with a scammer.

Visit SCAMwatch to find out how scams work, how to protect yourself and what to do if you've been scammed: www.scamwatch.gov.au

2015 campaign—‘Get smarter with your data’

The Taskforce's 2015 Fraud Week campaign, ‘Get smarter with your data’, will run from Monday 18 May to Sunday 24 May and focus on identity theft. The 2015 campaign will be asking Australians to carefully consider how they might better protect their personal information.

Scammers are using all sorts of tricks to convince people to part with their personal details or money. So many of the scams reported to the ACCC are underpinned by some aspect of identity fraud. Fake trader websites, classified advertisement scams, investment scams, online dating scams and charity scams, to name a few. All of these scams rely on convincing their victims they are who they say they are.

Scammers are also after your details to sell to other scammers or commit fraud themselves. Having established a fake identity, fraudsters can go on to purchase goods using stolen credit card details, set up bank accounts, take out loans or engage in money laundering, all in your name.

The key message of the campaign is ‘Get smarter with your data’ and asks Australians to think twice before disclosing their personal information.

7.2 The International Consumer Protection and Enforcement Network

The International Consumer Protection and Enforcement Network (ICPEN) is a network comprised of over 50 governmental consumer protection authorities around the globe. It is a network through which authorities can cooperatively share information and look at combating arising consumer problems with cross-border transactions in goods and services, such as e-commerce fraud and international scams. ICPEN encourages international cooperation among law enforcement agencies.

ICPEN's Global Fraud Prevention education initiative aims to inform consumers about fraud and raise awareness of scams through targeted events and activities. The ACCC participates as part of its national Fraud Week campaign with the Australasian Consumer Fraud Taskforce.

An important ICPEN initiative is econsumer.gov, a website portal featuring a global online complaints mechanism, which consumers can use to report complaints about online and related transactions with foreign companies. The site was developed in 2001 as a response to the challenges of multinational internet fraud. It is available in eight languages. The portal also provides consumers with tips on how they may be able to resolve issues and provides contacts for alternative dispute resolution services in ICPEN member jurisdictions, including Australia.

Collaboration with overseas law enforcement agencies to disrupt scams

Queensland and Western Australia (WA) Police work closely with overseas law enforcement agencies to disrupt scams targeting locals.

In 2013 WA authorities worked closely with the Nigerian Economic and Financial Crimes Commission (NEFCC) following the tragic circumstances that befell a WA woman. The woman was found dead after travelling overseas to meet a Nigerian that she met online. Before her death, the victim had lost more than \$100 000 to the scammer.

The NEFCC recognises the prevalence of scams activity that originates out of Nigeria and is committed to working with other law enforcement agencies, including Australian authorities, to identify and prosecute local perpetrators.

In January 2014 this collaborative effort culminated in the Nigerian scammer being arrested on fraud charges in relation to this crime. In July of 2014 the man was brought to court for conspiracy and obtaining the sum of \$90 000 from an Australian woman under false pretenses. He pleaded not guilty to the charges and his lawyer asked the court to grant him bail but the court remanded him in custody. The South African police investigating the matter believe he also had a hand in the demise of the WA woman.

7.3 Australian Transaction Reports and Analysis Centre partnership

Since 2006 the ACCC has been a partner agency with the Australian Transaction Reports and Analysis Centre (AUSTRAC) as authorised under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Clth).

AUSTRAC is Australia's anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit. It works with domestic partners including law enforcement, revenue, regulatory and social justice agencies, and their international counterparts. Intelligence from AUSTRAC is used as part of the scams disruption work undertaken by the ACCC.

AUSTRAC data also informs the ACCC's Scam Disruption project where letters are sent to New South Wales and Australian Capital Territory residents that send funds to high risk jurisdictions—see section 3.1 for more information.

More information about AUSTRAC can be found at: www.austrac.gov.au.

7.4 Australian Cybercrime Online Reporting Network (ACORN)

On 26 November 2014 the Australian Government launched the Australian Cybercrime Online Reporting Network (ACORN) as part of its response to cybercrime.

ACORN is a national online system that allows the public to securely report instances of cybercrime. It is a key initiative under the National Plan to Combat Cybercrime, which sets out how Australian agencies, including the ACCC, are working together to make Australia a harder target for cybercriminals.

The ACORN has been designed to make it easier to report cybercrime and help develop a better understanding of the cybercrime affecting Australians. Intelligence and threat assessments on ACORN data are assessed by the Australian Crime Commission to assist in the development of a clearer national picture. The system also refers reports to law enforcement and government agencies to help them respond quickly to acts of cybercrime.

The ACCC is working to ensure that contacts about online scams received through ACORN and SCAMwatch form part of the national data set of cybercrime. SCAMwatch will continue to receive contacts from the public and to provide educational information and advice to the public on online scams.

Further information about ACORN is available at www.acorn.gov.au.

Appendix 1: Glossary of scam terms

Attempts to gain your personal information (fake bank or telco, computer hacking, ID theft)

Hacking

Scammers often use information obtained from phishing scams and other sources to hack into your email, banking or social media accounts. Once they have compromised your accounts, they can change passwords preventing you from accessing your accounts. Scammers often then send out messages impersonating you either directing people to fake websites or claiming that you are stuck overseas and requesting that your friends send money.

Phishing

'Phishing' refers to emails, text messages or websites that trick people into giving out their personal and banking information. These messages pretend to come from legitimate businesses, normally banks or other financial institutions or telecommunications providers. The scammers try to obtain valuable personal information like passwords, bank account or credit card numbers.

ID theft involving spam or phishing

This category is used to capture data where ID theft involving spam or phishing has occurred and a fake identity has been created.

Buying, selling or donating (classifieds, business listings, auction, health, fake business etc.)

Classified scams

Scammers use online classified and auction sites to advertise (often popular) products for sale at cheap prices. They will ask for payment up front and often claim to be overseas. The scammer may try to gain your trust with false but convincing documents and elaborate stories.

Fake charity scams

Scammers take advantage of natural disasters and other events by impersonating charities and requesting donations.

Fake trader websites

Fake websites offer goods for sale, often advertised at very cheap prices. They will accept payments from you but never deliver the items ordered. These websites often look very similar or almost identical to genuine retail sites.

False billing

A false billing scam is a scam that targets small businesses, trying to bill them for a service such as advertising. The scam might come as a proposal for a subscription disguised as an invoice. Another common approach used by scammers is to ring a firm asking to confirm details of a service that they claim has already been booked. The scammer might try to convince them that they have used the scammer's product in the past. Scammers might also try to intimidate businesses by threatening legal action.

Health and medical products

These scams try to make money by exploiting people who have a medical condition or who are worried about their health. The scammers offer solutions or cures where none exist or promise to simplify complex health treatments.

Mobile premium services

These scams try to attract you with offers for 'free' goods, asking you to enter an online competition or complete a survey. Scammers ask for your mobile number to complete this task. What you may not realise is that by accepting the offer, you are actually subscribing to a service that will keep sending you SMS messages and add the cost of these to your phone bill.

Overpayment scams

Scammers target people selling over online classified or auction sites. The scammer will make a payment for a greater amount than the price of the good. The scammer will invent an excuse for the overpayment e.g. the extra money is meant to cover the fees of an agent or extra shipping costs. The scammer will then ask you to refund the excess amount or forward it on to a third party, usually through online bank transfer or wire transfer. The scammer is hoping to gain payment before you discover that the original payment is fraudulent.

Psychic and clairvoyant

Psychic and clairvoyant scammers approach you foreshadowing a positive upcoming event or claiming that you are in some sort of trouble and offering a solution. This 'solution' could be winning lottery numbers, a lucky charm, the removal of a 'curse' or 'jinx', or ongoing 'protection'. The scammer will tell you that they can help you in return for a fee/s. If you refuse to pay, some scammers may threaten to invoke a curse or bad luck charm.

Remote access scams

The scammer contacts you claiming that your computer is infected and that they need remote access to check. The scammer may try to convince you to purchase anti-virus software to remove the infection. The fee may be a one-off payment or an ongoing subscription.

Other buying and selling scams

Any other scam not identified in the preceding nine scam categories where something is supposedly bought or sold. Preference is given to classifying scams into more specific categories where this is possible.

Dating and Romance (including Adult Services)

Dating and romance scams

Dating and romance scams are particularly convincing because they appeal to your romantic or compassionate side. They play on emotional triggers to get you to provide money, gifts or personal details.

Jobs and investment (sport, high return, pyramid scheme, employment)

Computing prediction software and sports investment schemes

Sports investment schemes can include computer prediction (betting software) or betting syndicates. Salespeople try to convince you that their fool proof system can guarantee you a profit on sporting events like football or horseracing. These schemes are often camouflaged as legitimate investments.

Investment schemes

These scams use highly sophisticated websites to trick consumers into thinking investment offers are legitimate. In many cases scammers contact you through unsolicited phone calls and emails. Scammers claim that the investment will provide attractive returns and use high pressure sales tactics.

Job and employment

Job and employment scams target people looking for a new job or a change of job. They often promise an inflated income (sometimes they even guarantee it) for little effort or they demand an upfront payment before the job is yours. These scams can involve you engaging in money laundering, which is a crime.

Pyramid schemes

Pyramid schemes are illegal and very risky 'get-rich-quick' schemes. Promoters at the top of the pyramid make their money by having people join the scheme. In a typical pyramid scheme, a member pays to join. If the only returns from a scheme are entirely or substantially reliant on the member convincing other people to join up, then it is an illegal pyramid scheme.

Other business, employment and investment scams

Other business, employment and investment scams.

Threats and extortion (malware and software by email, malware and software by phone, hitman etc.)

Hitman scams

Hitman scams involve scammers sending death threats claiming to be from 'hitmen' hired to kill you unless you send them cash.

Ransomware and malware

Ransomware and malware involves a scammer placing harmful software onto your computer. Malware can give scammers access to your computer, collect personal information or just cause damage to the computer. Often the malware will cause the computer to freeze or lock and scammers will demand a payment to have the computer unlocked. These scams can target both individuals and businesses.

Unexpected money (inheritance, helping a foreigner, fake government or bank, loan opportunity)

Inheritance scams

An inheritance scam is when a scammer contacts you unexpectedly to tell you that you've been left, or are entitled to claim, a large inheritance from a distant relative or wealthy benefactor who has died overseas. Scammers will often pose as a lawyer, banker or other foreign official and will advise that the deceased left no other beneficiaries.

Nigerian scams

A 'Nigerian' scam is a form of upfront payment or money transfer scam. They are called Nigerian scams because the first wave appeared to emerge from Nigeria. They now come from anywhere in the world. The scammers offer you a share in a large sum of money that they want to transfer out of their country for a range of reasons e.g. to release money trapped in central banks during civil wars or coups. Or they may tell you about massive inheritances that are difficult to access because of government restrictions or taxes.

Reclaim scams

Scammers contact a victim pretending to be from the government, utilities, banks or other well known entities and ask for an upfront fee to reclaim money. Reasons this money is owed can include overcharged bank fees, tax refunds or compensation.

Other upfront payment and advanced fee frauds

Scammers commonly try to get you make advance payments for promises that never materialise. These promises vary but can include providing you with a loan or promising to return funds previously lost in an early scam.

Unexpected prizes (lottery, travel, scratchie)

Scratchie scams

Scratchie scams involve receiving a package in the mail which will commonly contain colourful travel brochures and a number of scratchie cards. One card will always be a winner, although not always first prize. When you call the number provided in the package, the scammer will ask for fees or taxes to be paid usually via a wire transfer service.

Travel prize scams

Travel prize scams often involve scammers claiming you have won a free holiday or travel related products. In fact all you have won is the chance to purchase accommodation or flight vouchers, which often fail to disclose that other terms apply and may involve additional costs, limited availability or other restrictions.

Unexpected prize and lottery scams

The scammer may tell you that you have won something substantial (such as a large sum of money, or shopping vouchers) and that all you have to do is send money or provide personal information to claim the winnings. Alternatively scammers may be asking you to buy into a fake lottery or competition.

Appendix 2: Scam tables by state and territory

Where possible the ACCC collects data about the geographic location of people reporting scams. Appendix 2 provides a breakdown of 2014 scam categories by state and territory.

Overall New South Wales received the greatest number of scam reports followed by Queensland and Victoria. Contacts for the remaining states and territories were below 10 per cent.

In addition to the above figures the ACCC received 1432 scam contacts from people based overseas, and a further 324 where their location was not provided, representing less than 2 per cent of total contacts.

Australian Capital Territory

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|--------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Dating and romance | \$1 182 520 | 68 | 31 | 19 | 12 | 37 | 46% |
| Computer prediction software and sports investment schemes | \$235 800 | 12 | 6 | 2 | 4 | 6 | 50% |
| Other buying and selling scams | \$155 206 | 225 | 70 | 68 | 2 | 155 | 31% |
| Hacking | \$128 771 | 154 | 14 | 11 | 3 | 140 | 9% |
| Fake trader websites | \$84 483 | 64 | 45 | 43 | 2 | 19 | 70% |
| Job and employment | \$58 725 | 52 | 10 | 8 | 2 | 42 | 19% |
| Scratchie scams | \$58 000 | 78 | 3 | 2 | 1 | 75 | 4% |
| Investment schemes | \$54 906 | 29 | 7 | 4 | 3 | 22 | 24% |
| Reclaim scams | \$42 648 | 478 | 6 | 5 | 1 | 472 | 1% |
| Unexpected prize and lottery scams | \$42 094 | 128 | 7 | 6 | 1 | 121 | 5% |
| Classified scams | \$40 073 | 124 | 36 | 36 | | 88 | 29% |
| Inheritance scams | \$33 900 | 145 | 3 | 2 | 1 | 142 | 2% |
| Other upfront payment and advanced fee frauds | \$31 738 | 124 | 15 | 15 | | 109 | 12% |
| Remote access scams | \$28 359 | 253 | 23 | 23 | | 230 | 9% |
| Overpayment scams | \$21 171 | 33 | 8 | 7 | 1 | 25 | 24% |
| Pyramid schemes | \$20 500 | 8 | 2 | 1 | 1 | 6 | 25% |
| False billing | \$14 139 | 89 | 10 | 10 | | 79 | 11% |
| ID theft involving spam or phishing | \$5 610 | 253 | 11 | 11 | | 242 | 4% |
| Other business, employment and investment scams | \$5 563 | 30 | 6 | 6 | | 24 | 20% |
| Phishing | \$4 255 | 448 | 10 | 10 | | 438 | 2% |
| Travel prize scams | \$1 254 | 126 | 2 | 2 | | 124 | 2% |
| Nigerian scams | \$1 155 | 24 | 1 | 1 | | 23 | 4% |
| Ransomware and malware | \$1 053 | 100 | 6 | 6 | | 94 | 6% |
| (blank) | \$701 | 24 | 1 | 1 | | 23 | 4% |
| Fake charity scams | \$555 | 16 | 3 | 3 | | 13 | 19% |
| Health and medical products | \$470 | 9 | 5 | 5 | | 4 | 56% |
| Mobile premium services | \$370 | 10 | 4 | 4 | | 6 | 40% |
| Hitman scams | \$269 | 17 | 1 | 1 | | 16 | 6% |
| Total | \$2 254 288 | 3 121 | 346 | 312 | 34 | 2 775 | 11% |

New South Wales

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|---------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Dating and romance | \$8 911 557 | 656 | 263 | 162 | 101 | 393 | 40% |
| Investment schemes | \$3 345 266 | 256 | 77 | 25 | 52 | 179 | 30% |
| Inheritance scams | \$2 539 055 | 1 227 | 28 | 14 | 14 | 1 199 | 2% |
| Computer prediction software and sports investment schemes | \$2 118 497 | 126 | 66 | 29 | 37 | 60 | 52% |
| Nigerian scams | \$737 160 | 315 | 23 | 15 | 8 | 292 | 7% |
| Other buying and selling scams | \$684 432 | 1 956 | 631 | 619 | 12 | 1 325 | 32% |
| Other upfront payment and advanced fee frauds | \$663 124 | 1 267 | 182 | 165 | 17 | 1 085 | 14% |
| Other business, employment and investment scams | \$646 988 | 266 | 49 | 39 | 10 | 217 | 18% |
| Unexpected prize and lottery scams | \$586 668 | 962 | 72 | 66 | 6 | 890 | 7% |
| Classified scams | \$376 901 | 958 | 227 | 219 | 8 | 731 | 24% |
| Job and employment | \$355 159 | 493 | 80 | 73 | 7 | 413 | 16% |
| Fake trader websites | \$340 475 | 649 | 410 | 402 | 8 | 239 | 63% |
| Remote access scams | \$309 198 | 2 559 | 211 | 204 | 7 | 2 348 | 8% |
| Reclaim scams | \$210 172 | 4 422 | 69 | 67 | 2 | 4 353 | 2% |
| Hacking | \$210 018 | 1 240 | 93 | 87 | 6 | 1 147 | 8% |
| Ransomware and malware | \$203 282 | 804 | 34 | 30 | 4 | 770 | 4% |
| Phishing | \$191 986 | 4 410 | 78 | 75 | 3 | 4 332 | 2% |
| False billing | \$123 965 | 778 | 84 | 81 | 3 | 694 | 11% |
| ID theft involving spam or phishing | \$107 184 | 2 465 | 111 | 109 | 2 | 2 354 | 5% |
| Overpayment scams | \$95 547 | 388 | 53 | 53 | | 335 | 14% |
| Scratchie scams | \$58 902 | 90 | 5 | 3 | 2 | 85 | 6% |
| Hitman scams | \$57 513 | 62 | 7 | 6 | 1 | 55 | 11% |
| Travel prize scams | \$44 832 | 569 | 31 | 30 | 1 | 538 | 5% |
| Pyramid schemes | \$41 692 | 66 | 10 | 8 | 2 | 56 | 15% |
| Fake charity scams | \$26 573 | 208 | 34 | 33 | 1 | 174 | 16% |
| Health and medical products | \$21 732 | 122 | 55 | 55 | | 67 | 45% |
| Psychic and clairvoyant | \$13 147 | 15 | 8 | 8 | | 7 | 53% |
| (blank) | \$10 830 | 236 | 10 | 10 | | 226 | 4% |
| Mobile premium services | \$1 732 | 82 | 33 | 33 | | 49 | 40% |
| Total | \$23 033 587 | 27 647 | 3 034 | 2 720 | 314 | 24 613 | 11% |

Northern Territory

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Dating and romance | \$101 485 | 23 | 10 | 7 | 3 | 13 | 43% |
| Computer prediction software and sports investment schemes | \$62 990 | 4 | 2 | | 2 | 2 | 50% |
| Classified scams | \$48 200 | 54 | 13 | 12 | 1 | 41 | 24% |
| Other upfront payment and advanced fee frauds | \$25 031 | 53 | 18 | 18 | | 35 | 34% |
| Hacking | \$20 669 | 53 | 7 | 6 | 1 | 46 | 13% |
| Other business, employment and investment scams | \$18 300 | 8 | 3 | 2 | 1 | 5 | 38% |
| Remote access scams | \$17 042 | 63 | 6 | 5 | 1 | 57 | 10% |
| Other buying and selling scams | \$15 286 | 88 | 27 | 27 | | 61 | 31% |
| Phishing | \$7 900 | 115 | 2 | 2 | | 113 | 2% |
| Fake trader websites | \$4 988 | 17 | 9 | 9 | | 8 | 53% |
| Nigerian scams | \$4 300 | 10 | 2 | 2 | | 8 | 20% |
| ID theft involving spam or phishing | \$4 210 | 63 | 4 | 4 | | 59 | 6% |
| Travel prize scams | \$3 357 | 21 | 4 | 4 | | 17 | 19% |
| Reclaim scams | \$2 480 | 84 | 2 | 2 | | 82 | 2% |
| Overpayment scams | \$2 000 | 10 | 1 | 1 | | 9 | 10% |
| Unexpected prize and lottery scams | \$1 797 | 49 | 4 | 4 | | 45 | 8% |
| Ransomware and malware | \$1 306 | 26 | 3 | 3 | | 23 | 12% |
| Job and employment | \$1 210 | 13 | 2 | 2 | | 11 | 15% |
| Hitman scams | \$700 | 2 | 1 | 1 | | 1 | 50% |
| False billing | \$522 | 28 | 1 | 1 | | 27 | 4% |
| Investment schemes | \$228 | 7 | 2 | 2 | | 5 | 29% |
| (blank) | \$200 | 10 | 1 | 1 | | 9 | 10% |
| Health and medical products | \$170 | 4 | 1 | 1 | | 3 | 25% |
| Mobile premium services | \$40 | 2 | 1 | 1 | | 1 | 50% |
| Fake charity scams | \$22 | 5 | 1 | 1 | | 4 | 20% |
| Inheritance scams | \$- | 35 | 0 | | | 35 | 0% |
| Pyramid schemes | \$- | 3 | 0 | | | 3 | 0% |
| Total | \$344 433 | 850 | 127 | 118 | 9 | 723 | 15% |

Queensland

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|---------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Dating and romance | \$5 780 010 | 544 | 234 | 147 | 87 | 310 | 43% |
| Investment schemes | \$3 007 622 | 186 | 76 | 30 | 46 | 110 | 41% |
| Computer prediction software and sports investment schemes | \$2 511 220 | 111 | 60 | 29 | 31 | 51 | 54% |
| Nigerian scams | \$797 252 | 251 | 18 | 11 | 7 | 233 | 7% |
| Other buying and selling scams | \$739 094 | 1633 | 556 | 536 | 20 | 1077 | 34% |
| Classified scams | \$661 815 | 823 | 159 | 140 | 19 | 664 | 19% |
| Hacking | \$647 297 | 936 | 72 | 68 | 4 | 864 | 8% |
| Other upfront payment and advanced fee frauds | \$528 360 | 941 | 128 | 118 | 10 | 813 | 14% |
| Ransomware and malware | \$506 590 | 566 | 32 | 27 | 5 | 534 | 6% |
| Other business employment and investment scams | \$505 984 | 194 | 45 | 33 | 12 | 149 | 23% |
| Remote access scams | \$344 403 | 1813 | 182 | 174 | 8 | 1631 | 10% |
| Unexpected prize and lottery scams | \$272 501 | 696 | 57 | 52 | 5 | 639 | 8% |
| Inheritance scams | \$239 625 | 1036 | 14 | 6 | 8 | 1022 | 1% |
| Fake trader websites | \$213 831 | 397 | 257 | 252 | 5 | 140 | 65% |
| Job and employment | \$210 473 | 435 | 50 | 43 | 7 | 385 | 11% |
| ID theft involving spam or phishing | \$183 087 | 1750 | 95 | 89 | 6 | 1655 | 5% |
| Hitman scams | \$150 728 | 60 | 13 | 10 | 3 | 47 | 22% |
| Overpayment scams | \$138 744 | 361 | 38 | 35 | 3 | 323 | 11% |
| Pyramid schemes | \$122 285 | 50 | 11 | 10 | 1 | 39 | 22% |
| Scratchie scams | \$102 586 | 137 | 11 | 6 | 5 | 126 | 8% |
| Fake charity scams | \$96 489 | 169 | 23 | 22 | 1 | 146 | 14% |
| Reclaim scams | \$89 471 | 3979 | 48 | 47 | 1 | 3931 | 1% |
| Phishing | \$77 372 | 2801 | 71 | 69 | 2 | 2730 | 3% |
| False billing | \$50 660 | 653 | 71 | 71 | | 582 | 11% |
| Travel prize scams | \$18 703 | 371 | 15 | 15 | | 356 | 4% |
| Mobile premium services | \$12 497 | 60 | 17 | 16 | 1 | 43 | 28% |
| Health and medical products | \$10 034 | 91 | 46 | 46 | | 45 | 51% |
| (blank) | \$5 637 | 161 | 6 | 6 | | 155 | 4% |
| Psychic and clairvoyant | \$865 | 15 | 3 | 3 | | 12 | 20% |
| Total | \$18 025 235 | 21 220 | 2 408 | 2 111 | 297 | 18 812 | 11% |

South Australia

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|-------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Investment schemes | \$804 042 | 65 | 28 | 10 | 18 | 37 | 43% |
| Dating and romance | \$801 848 | 142 | 50 | 39 | 11 | 92 | 35% |
| Other upfront payment and advanced fee frauds | \$467 623 | 287 | 42 | 37 | 5 | 245 | 15% |
| Computer prediction software and sports investment schemes | \$397 538 | 40 | 20 | 9 | 11 | 20 | 50% |
| Fake trader websites | \$185 471 | 153 | 92 | 88 | 4 | 61 | 60% |
| Other buying and selling scams | \$145 860 | 475 | 164 | 161 | 3 | 311 | 35% |
| Inheritance scams | \$109 296 | 390 | 8 | 6 | 2 | 382 | 2% |
| Classified scams | \$63 903 | 251 | 61 | 59 | 2 | 190 | 24% |
| Hacking | \$50 383 | 313 | 17 | 15 | 2 | 296 | 5% |
| False billing | \$47 808 | 270 | 33 | 32 | 1 | 237 | 12% |
| Remote access scams | \$46 029 | 762 | 65 | 64 | 1 | 697 | 9% |
| Reclaim scams | \$43 597 | 995 | 26 | 26 | | 969 | 3% |
| Phishing | \$38 361 | 1048 | 29 | 29 | | 1 019 | 3% |
| Unexpected prize and lottery scams | \$37 309 | 336 | 28 | 27 | 1 | 308 | 8% |
| Other business, employment and investment scams | \$22 571 | 53 | 6 | 5 | 1 | 47 | 11% |
| Scratchie scams | \$21 100 | 96 | 6 | 6 | | 90 | 6% |
| Job and employment | \$19 638 | 109 | 12 | 12 | | 97 | 11% |
| Overpayment scams | \$17 636 | 94 | 15 | 15 | | 79 | 16% |
| ID theft involving spam or phishing | \$15 690 | 648 | 37 | 37 | | 611 | 6% |
| Ransomware and malware | \$6 097 | 203 | 8 | 8 | | 195 | 4% |
| Travel prize scams | \$2 766 | 71 | 4 | 4 | | 67 | 6% |
| Health and medical products | \$1 227 | 27 | 7 | 7 | | 20 | 26% |
| Mobile premium services | \$392 | 16 | 7 | 7 | | 9 | 44% |
| (blank) | \$380 | 65 | 3 | 3 | | 62 | 5% |
| Psychic and clairvoyant | \$344 | 5 | 2 | 2 | | 3 | 40% |
| Pyramid schemes | \$234 | 12 | 1 | 1 | | 11 | 8% |
| Fake charity scams | \$25 | 42 | 2 | 2 | | 40 | 5% |
| Nigerian scams | \$2 | 85 | 1 | 1 | | 84 | 1% |
| Hitman scams | \$- | 10 | | | | 10 | 0% |
| Total | \$3 347 170 | 7063 | 774 | 712 | 62 | 6289 | 11% |

Tasmania

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|--------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Investment schemes | \$804 042 | 65 | 28 | 10 | 18 | 37 | 43% |
| Dating and romance | \$801 848 | 142 | 50 | 39 | 11 | 92 | 35% |
| Other upfront payment and advanced fee frauds | \$467 623 | 287 | 42 | 37 | 5 | 245 | 15% |
| Computer prediction software and sports investment schemes | \$397 538 | 40 | 20 | 9 | 11 | 20 | 50% |
| Fake trader websites | \$185 471 | 153 | 92 | 88 | 4 | 61 | 60% |
| Other buying and selling scams | \$145 860 | 475 | 164 | 161 | 3 | 311 | 35% |
| Inheritance scams | \$109 296 | 390 | 8 | 6 | 2 | 382 | 2% |
| Classified scams | \$63 903 | 251 | 61 | 59 | 2 | 190 | 24% |
| Hacking | \$50 383 | 313 | 17 | 15 | 2 | 296 | 5% |
| False billing | \$47 808 | 270 | 33 | 32 | 1 | 237 | 12% |
| Remote access scams | \$46 029 | 762 | 65 | 64 | 1 | 697 | 9% |
| Reclaim scams | \$43 597 | 995 | 26 | 26 | | 969 | 3% |
| Phishing | \$38 361 | 1 048 | 29 | 29 | | 1019 | 3% |
| Unexpected prize and lottery scams | \$37 309 | 336 | 28 | 27 | 1 | 308 | 8% |
| Other business employment and investment scams | \$22 571 | 53 | 6 | 5 | 1 | 47 | 11% |
| Scratchie scams | \$21 100 | 96 | 6 | 6 | | 90 | 6% |
| Job and employment | \$19 638 | 109 | 12 | 12 | | 97 | 11% |
| Overpayment scams | \$17 636 | 94 | 15 | 15 | | 79 | 16% |
| ID theft involving spam or phishing | \$15 690 | 648 | 37 | 37 | | 611 | 6% |
| Ransomware and malware | \$6 097 | 203 | 8 | 8 | | 195 | 4% |
| Travel prize scams | \$2 766 | 71 | 4 | 4 | | 67 | 6% |
| Health and medical products | \$1 227 | 27 | 7 | 7 | | 20 | 26% |
| Mobile premium services | \$392 | 16 | 7 | 7 | | 9 | 44% |
| (blank) | \$380 | 65 | 3 | 3 | | 62 | 5% |
| Psychic and clairvoyant | \$344 | 5 | 2 | 2 | | 3 | 40% |
| Pyramid schemes | \$234 | 12 | 1 | 1 | | 11 | 8% |
| Fake charity scams | \$25 | 42 | 2 | 2 | | 40 | 5% |
| Nigerian scams | \$2 | 85 | 1 | 1 | | 84 | 1% |
| Hitman scams | \$- | 10 | | | | 10 | 0% |
| Total | \$3 347 170 | 7 063 | 774 | 712 | 62 | 6 289 | 11% |

Victoria

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|---------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Dating and romance | \$6 811 791 | 496 | 228 | 134 | 94 | 268 | 46% |
| Computer prediction software and sports investment schemes | \$2 662 277 | 99 | 58 | 29 | 29 | 41 | 59% |
| Investment schemes | \$2 550 099 | 214 | 60 | 25 | 35 | 154 | 28% |
| Hacking | \$1 136 289 | 1 255 | 89 | 82 | 7 | 1 166 | 7% |
| Overpayment scams | \$1 061 894 | 237 | 42 | 37 | 5 | 195 | 18% |
| Inheritance scams | \$899 970 | 825 | 25 | 8 | 17 | 800 | 3% |
| Other business employment and investment scams | \$882 195 | 237 | 52 | 42 | 10 | 185 | 22% |
| Other buying and selling scams | \$656 283 | 1 462 | 536 | 524 | 12 | 926 | 37% |
| Fake trader websites | \$606 821 | 472 | 323 | 313 | 10 | 149 | 68% |
| Unexpected prize and lottery scams | \$467 939 | 623 | 56 | 47 | 9 | 567 | 9% |
| Psychic and clairvoyant | \$450 008 | 7 | 2 | 1 | 1 | 5 | 29% |
| Classified scams | \$387 043 | 575 | 163 | 154 | 9 | 412 | 28% |
| Remote access scams | \$343 918 | 2 492 | 212 | 207 | 5 | 2 280 | 9% |
| Other upfront payment and advanced fee frauds | \$321 312 | 812 | 134 | 127 | 7 | 678 | 17% |
| Nigerian scams | \$197 570 | 171 | 21 | 14 | 7 | 150 | 12% |
| Job and employment | \$156 875 | 421 | 50 | 46 | 4 | 371 | 12% |
| ID theft involving spam or phishing | \$155 604 | 1 815 | 100 | 96 | 4 | 1 715 | 6% |
| False billing | \$135 514 | 495 | 64 | 62 | 2 | 431 | 13% |
| Reclaim scams | \$127 184 | 2 538 | 59 | 56 | 3 | 2 479 | 2% |
| Phishing | \$126 726 | 2 604 | 69 | 66 | 3 | 2 535 | 3% |
| Ransomware and malware | \$106 818 | 528 | 45 | 42 | 3 | 483 | 9% |
| Hitman scams | \$57 618 | 55 | 4 | 2 | 2 | 51 | 7% |
| Scratchie scams | \$36 608 | 111 | 4 | 2 | 2 | 107 | 4% |
| Pyramid schemes | \$27 300 | 63 | 7 | 6 | 1 | 56 | 11% |
| Health and medical products | \$18 685 | 87 | 39 | 39 | | 48 | 45% |
| Fake charity scams | \$15 390 | 121 | 23 | 23 | | 98 | 19% |
| Travel prize scams | \$7 249 | 345 | 10 | 10 | | 335 | 3% |
| Mobile premium services | \$2 815 | 58 | 23 | 23 | | 35 | 40% |
| (blank) | \$1 716 | 155 | 3 | 3 | | 152 | 2% |
| Total | \$20 411 511 | 19 373 | 2 501 | 2 220 | 281 | 16 872 | 13% |

Western Australia

| Scam category Level 2 | Amount reported lost | Contacts | Contacts reporting loss | Less than \$10k lost | Greater than \$10k lost | Contacts reporting no loss | Conversion rate |
|--|----------------------|--------------|-------------------------|----------------------|-------------------------|----------------------------|-----------------|
| Dating and romance | \$2 241 817 | 266 | 96 | 59 | 37 | 170 | 36% |
| Investment schemes | \$1 991 815 | 117 | 40 | 13 | 27 | 77 | 34% |
| Computer prediction software and sports investment schemes | \$947 738 | 76 | 34 | 13 | 21 | 42 | 45% |
| Other upfront payment and advanced fee frauds | \$536 160 | 401 | 67 | 59 | 8 | 334 | 17% |
| Other buying and selling scams | \$434 351 | 797 | 307 | 297 | 10 | 490 | 39% |
| Reclaim scams | \$290 763 | 884 | 26 | 20 | 6 | 858 | 3% |
| ID theft involving spam or phishing | \$286 251 | 781 | 42 | 36 | 6 | 739 | 5% |
| Classified scams | \$207 481 | 329 | 89 | 82 | 7 | 240 | 27% |
| Unexpected prize and lottery scams | \$168 524 | 329 | 25 | 21 | 4 | 304 | 8% |
| Fake trader websites | \$137 290 | 212 | 150 | 147 | 3 | 62 | 71% |
| Overpayment scams | \$110 841 | 123 | 22 | 19 | 3 | 101 | 18% |
| Phishing | \$90 309 | 1 102 | 21 | 19 | 2 | 1 081 | 2% |
| Remote access scams | \$77 928 | 563 | 51 | 48 | 3 | 512 | 9% |
| Other business employment and investment scams | \$69 788 | 107 | 14 | 12 | 2 | 93 | 13% |
| Nigerian scams | \$61 930 | 118 | 7 | 5 | 2 | 111 | 6% |
| Inheritance scams | \$34 370 | 497 | 4 | 2 | 2 | 493 | 1% |
| Job and employment | \$31 944 | 183 | 17 | 17 | | 166 | 9% |
| False billing | \$30 922 | 263 | 34 | 34 | | 229 | 13% |
| Psychic and clairvoyant | \$30 000 | 1 | 1 | | 1 | | 100% |
| Travel prize scams | \$27 074 | 101 | 12 | 11 | 1 | 89 | 12% |
| Ransomware and malware | \$26 709 | 214 | 16 | 15 | 1 | 198 | 7% |
| Hacking | \$21 799 | 357 | 20 | 19 | 1 | 337 | 6% |
| Health and medical products | \$16 616 | 42 | 28 | 28 | | 14 | 67% |
| Pyramid schemes | \$5 664 | 19 | 5 | 5 | | 14 | 26% |
| Scratchie scams | \$4 600 | 4 | 1 | 1 | | 3 | 25% |
| Mobile premium services | \$3 842 | 20 | 11 | 11 | | 9 | 55% |
| Hitman scams | \$2 520 | 46 | 4 | 4 | | 42 | 9% |
| Fake charity scams | \$2 260 | 73 | 12 | 12 | | 61 | 16% |
| (blank) | \$1 550 | 59 | 3 | 3 | | 56 | 5% |
| Total | \$7 892 856 | 8 084 | 1 159 | 1 012 | 147 | 6 925 | 14% |

Appendix 3: SCAMwatch radars

Don't let weight loss scams ruin your resolve this New Year

January 2014: SCAMwatch is warning consumers to beware of weight loss scams when looking to fulfill a new year's resolution.

Computer virus scams now targeting smartphone and tablet users

January 2014: SCAMwatch is warning consumers to beware of scammers targeting their smartphones and tablet devices with the computer virus scam.

Alert update—'Yellow Pages' directory scam moves to a new website address, continues to target Australian businesses

January 2014: SCAMwatch is warning small businesses to continue to be alert to the fake 'Yellow Pages' business directory scam. The scammers are now operating a site registered in Austria, 'www.yellow-page-australia.at', after their previous site, 'www.yellow-page-australia.com', was shut down.

Looking for love online? Don't get scammed into a broken heart and empty wallet

February 2014: This Valentine's Day, SCAMwatch is warning Australians looking for a romantic connection online to beware of scammers seeking to steal their hearts and money.

Don't be fooled by a fake franchise

February 2014: SCAMwatch is warning people thinking about buying a franchise or small business to beware of exciting new franchise opportunities that may actually be scams.

Don't let scammers kick goals in the lead up to the 2014 FIFA World Cup

March 2014: SCAMwatch and FIFA are warning soccer fans seeking to buy tickets to the 2014 FIFA World Cup in Brazil to beware of websites selling fake tickets.

Scammers using videos of Malaysian Airlines Flight MH370 to spread malware

March 2014: SCAMwatch and Stay Smart Online are warning consumers interested in finding out more about the recent disappearance of Malaysia Airlines flight MH370 to be on guard when opening video footage about this event, as scammers are sending links infected with malware.

Scammers pretending to be from Telstra Technical Support continue cold-calling Australians

March 2014: SCAMwatch and Telstra are warning consumers to hang up the phone if they receive a call out of the blue from someone claiming there is a problem with their internet connection or computer.

Automated scam calls claiming to be from Qantas with bogus holiday win

April 2014: SCAMwatch and Qantas are warning people about automated calls from scammers posing as Qantas staff claiming that they've won a credit towards their next holiday.

Beware—energy bill scams on the rise

May 2014: SCAMwatch is warning consumers to be on the lookout for energy billing scams currently doing the rounds.

Don't let scammers 'tax' you this tax time

July 2014: SCAMwatch and the Australian Taxation Office (ATO) are urging consumers and small businesses to be aware of scammers taking advantage of the busy nature of tax time to target you.

Beware of scammers taking advantage of the Malaysia Airlines Flight MH17 tragedy

July 2014: SCAMwatch is warning Australians to be wary of scammers looking to take advantage of the Malaysia Airlines tragedy by setting up fake Facebook pages in the name of victims of the tragedy.

Beware of carbon tax repeal scams

August 2014: SCAMwatch is warning consumers and businesses to be aware of scammers looking to take advantage of the carbon tax repeal to steal your money.

Consumers with a disability—be on guard against scammers trying to take advantage of you

August 2014: SCAMwatch is warning consumers with a disability to be on guard against scams—unfortunately, scammers target people whom they think may be vulnerable to try and take advantage of them.

Indigenous consumers, watch out for scams—the top scams reported

September 2014: SCAMwatch is urging Indigenous consumers, especially those living in rural and remote communities, to be on the lookout for scammers trying to trick you into handing over your personal details or money.

Don't book a scammer's holiday

October 2014: SCAMwatch is warning would-be travelers to watch out for travel scams as scammers seek to take advantage of those looking for a hard-earned break.

Don't let the Grinch steal Christmas—watch out for scammers

November 2014: With Christmas just around the corner, SCAMwatch is reminding consumers to watch out for scammers taking advantage of the Christmas rush to leave you out of pocket and a present.

Appendix 4: Other scam-related educational materials

SCAMwatch

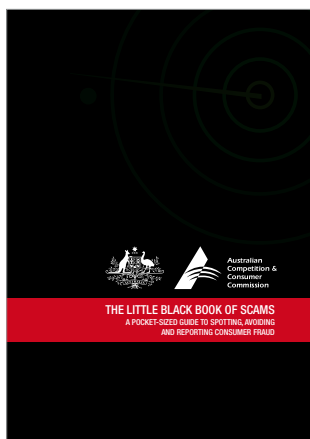


SCAMwatch website (www.scamwatch.gov.au)



SCAMwatch Twitter profile (@SCAMwatch_gov)
<https://twitter.com/scamwatch.gov>

Publications



The Little Black Book of Scams



ACCC Small business scams factsheet

Annual reports



Targeting scams: Report of the ACCC on scam activity—2009, 2010, 2011, 2012 and 2013 editions

2014 Fraud Week campaign resources

Campaign image

**KNOW WHO
YOU'RE
DEALING WITH**



Friend or foe? **Think twice before transferring money.**

Campaign web banner

**KNOW WHO
YOU'RE
DEALING WITH**



Think twice before transferring money
scamwatch.gov.au

AUSTRALASIAN
CONSUMER FRAUD
TASKFORCE

AN INITIATIVE OF THE STATE, TERRITORY AND
AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

Campaign button

**KNOW WHO
YOU'RE
DEALING WITH**



Think twice before transferring money
scamwatch.gov.au

